



Industria y
SUPERINTENDENCIA
República de Colombia
Ministerio de Comercio, Industria y Turismo

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
INVENTARIO

Delegatura de Propiedad Industrial
División de Nuevas Creaciones

SOLICITUD DE

PCT

**PATENTE DE INVENCION
PCT ENTRADA EN FASE NACIONAL**

21. EXPEDIENTE No.

09-20838

54. TITULO: SISTEMA Y METODO PARA AUTORIZACION DE
TRANSACCION

52. CLASIFICACION INTERNACIONAL: G06Q 20/00, G06F 17/30

71. SOLICITANTE: QPAY HOLDINGS LIMITED

DOMICILIO: 74 Wentworth Drive, Cabalaba, QLD 4157,
AUSTRALIA

74. APODERADO: Dra. MARGARITA CASTELLANOS A.

22. BOGOTA, D.C.,

- 2 MAR. 2009



No. 09-020838- -00000-0000

Fecha: 2009-03-02 14:53:24 Dep. 2020 NUECREACIONE
Tra. 11 PATENTEIYII Eve: 379 FASENACIONALII
Act. 411 PRESENTACION Folios: 134

FORMULARIO UNICO DE SOLICITUD DE PATENTES
PCT
ENTRADA EN FASE NACIONAL

SOLICITUD DE:

①

☒ Patente de Invención.

☐ Patente de Modelo de Utilidad.

☐ Capítulo I

☒ Capítulo II

②

SOLICITANTE (71)

Nombre: QPAY HOLDINGS LIMITED

Dirección: 74 Wentworth Drive
Capalaba, QLD 4157
AUSTRALIA

Nacionalidad o Domicilio: Capalaba,
AUSTRALIA
Lugar de Constitución: AUSTRALIA

Teléfono: Fax:
E-mail:

IDENTIFICACIÓN

C.C. ☐ NIT ☐

C.E. ☐ Otro ☐

Número Cual

③

REPRESENTANTE
O APODERADO

Nombre: MARGARITA CASTELLANOS A.

Dirección: CALLE 94A No. 7A-09

Teléfono: 610 7420 Fax: 610 0706

E-mail: info@castellanosyco.com

IDENTIFICACIÓN

C.C. ☒ NIT ☐

C.E. ☐ Otro ☐

Número 39'779.654 TPA 70.819

④

INVENTOR (ES) (72)

GREG WALTER
74 Wentworth Drive
Capalaba, QLD 4157
AUSTRALIA

⑤

PCT (86)

Solicitud Internacional No. PCT/AU2007/001076

Fecha 01/08/2007

Publicación Internacional No. WO 2008/014554 A1

Fecha 07/02/2008

⑥

Título (54)

SISTEMA Y METODO PARA AUTORIZACION DE TRANSACCION

⑦

Clasificación Internacional (51) G06Q 20/00; G06F 17/30

⑧

Prioridad

(33) País de Origen

(32) Fecha

(31) Número de Solicitud

SI ☒ NO ☐

AU

01/08/2006

2006904149

AU

01/02/2007

2007900469

⑨

Comprobantes de pago Nos. 09-16,630y 09-16,631

Fecha Marzo 2 de 2009

Instrucciones para el diligenciamiento del presente formulario, ver reverso de esta página.

10

Anexos

- ☒ Comprobante de pago de la tasa de presentación de la solicitud.
- ☐ Documento que acredita la existencia y representación legal cuando el solicitante sea persona jurídica.
- ☐ Poderes, si fuere el caso, junto con la sustitución del mismo a mi favor
- ☐ Documento de cesión del inventor al solicitante o a su causante.
- ☐ Declaraciones.
- ☒ Copia de la solicitud internacional (Resumen, descripción, reivindicaciones, dibujos).
- ☒ Traducción de la solicitud internacional al castellano (Resumen, descripción, reivindicaciones, dibujos).
- ☒ Copia del examen preliminar internacional efectuado por la Autoridad Internacional de Examen Preliminar (IPEA).
- ☐ Traducción del examen preliminar internacional efectuado por la IPEA.
- ☐ De ser el caso, copia del contrato de acceso.
- ☐ De ser el caso, documento que acredite la licencia o autorización de uso de conocimientos tradicionales de las comunidades indígenas.
- ☐ De ser el caso, certificado de depósito del material biológico.
- ☐ Arte final 12x12
- ☐ De ser el caso, información sobre otras solicitudes de patente o títulos obtenidos en el extranjero por el mismo titular o su causante, relacionadas parcial o totalmente con la invención de esta solicitud.
- ☐ De ser el caso, modificaciones efectuadas a la solicitud internacional.
- ☒ Otros Tarjeta Propietario y Extracto para la Publicación

11 FIGURA CARACTERISTICA:

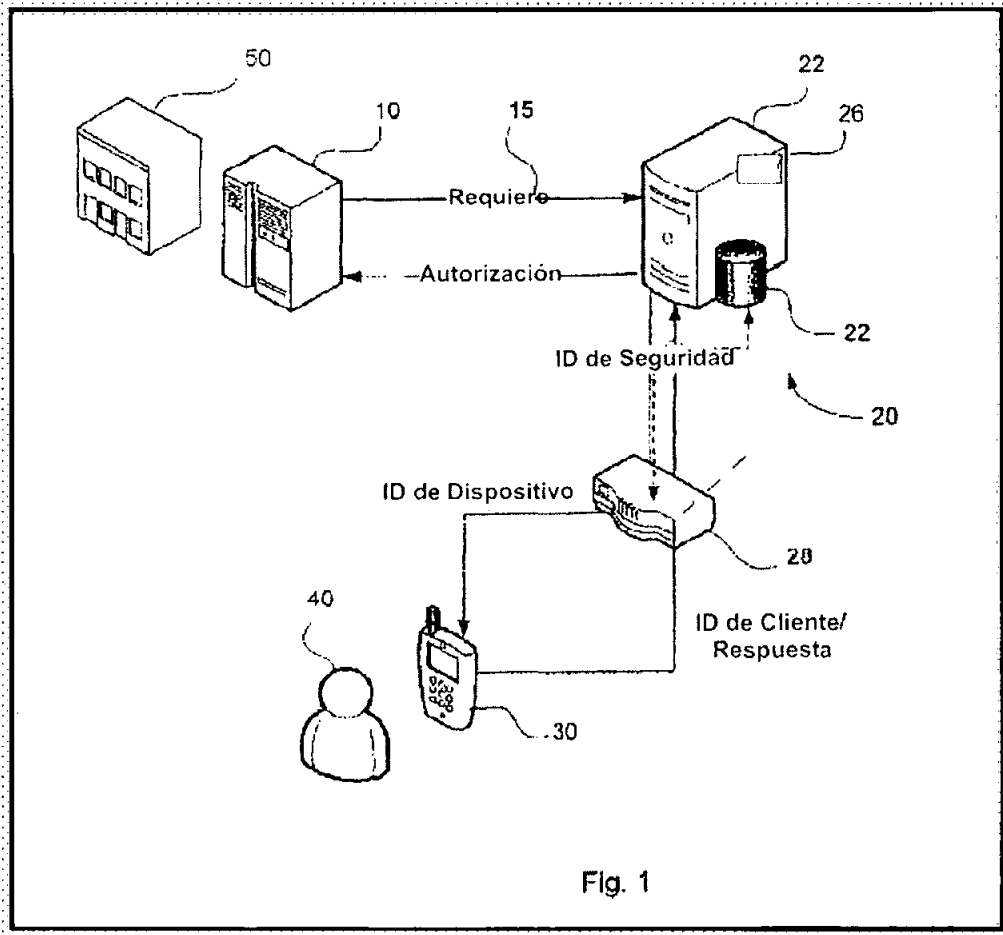


Fig. 1

12 Solicito la concesión de la patente,

NOMBRE: MARGARITA CASTELLANOS ABONDANO

FIRMA: *Margarita Castellanos*
C.C. No. 39'779.654 Usaquéen - TPA 70.819 C.S.J.

- 2 MAR. 2009

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
7 February 2008 (07.02.2008)

PCT

(10) International Publication Number
WO 2008/014554 A1

(51) International Patent Classification:
G06Q 20/00 (2006.01) *G06F 17/30* (2006.01)

(74) Agent: **WATERMARK PATENT & TRADEMARK ATTORNEYS**; 302 Burwood Road, Hawthorn, VIC 3122 (AU).

(21) International Application Number:
PCT/AU2007/001076

(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date: 1 August 2007 (01.08.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2006904149 1 August 2006 (01.08.2006) AU
2007900469 1 February 2007 (01.02.2007) AU

(84) Designated States (*unless otherwise indicated, for every kind of regional protection available*): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

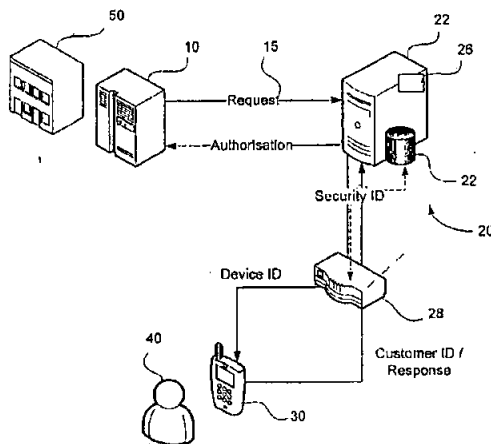
(71) Applicant (*for all designated States except US*): **QPAY HOLDINGS LIMITED** [AU/AU]; 74 Wentworth Drive, Capalaba, QLD 4157 (AU).

(72) Inventor; and

(75) Inventor/Applicant (*for US only*): **WALTER, Greg** [AU/AU]; 74 Wentworth Drive, Capalaba, QLD 4157 (AU).

Published:
— with international search report

(54) Title: TRANSACTION AUTHORISATION SYSTEM & METHOD



(57) Abstract: A transaction authorisation system (20) for allowing a customer (40) to authorise transactions relating to at least one customer (40) account associated with an institution (50), the system (20) including data storage means (24) for enabling access to identification data associated with the customer (40) and a remote communication device (RCD) (30) of the customer (40), and security identifier data associating the customer (40) account with the identification data. The system (20) also includes communication means (26) for receiving an authorisation request, which is referenced to the security identifier data, in relation to the transaction from the institution (50) and for enabling communication with the customer (40) via the RCD (30) to authorise a transaction on the customer (40) account. Data processing means (22) of the system (20) identify the customer (40) and RCD (30) using the identification data and determine if the transaction is authorised by the customer (40). The communication means (26) provides an indication, which is referenced to the security identifier data, to the institution (50) of whether or not the transaction is authorised by the customer (40).

WO 2008/014554 A1

TRANSACTION AUTHORISATION SYSTEM & METHOD**FIELD OF THE INVENTION**

The present invention relates to a system and method for the authorisation of transactions such as credit card purchases, bank transfers, and share
5 purchases, particularly in environments where remote payments for goods and services are made.

BACKGROUND OF THE INVENTION

Security of financial and other types of transactions is of great importance due to the relatively recent growth of threats such as phishing and pharming
10 which are intended to fraudulently acquire sensitive information, such as passwords, pin numbers and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Once such details are fraudulently acquired they are utilised to make financial payments or to misappropriate funds from financial accounts. The account holder is often without
15 any knowledge of these fraudulent transactions until after they have been concluded and it is too late to intervene. It is desirable, therefore, to seek authorisation of transactions from a customer before transactions are concluded by the financial institution.

In current systems used to authorise financial transactions, it is difficult and
20 often impossible to obtain a firm guarantee that the person initiating the transaction is the account holder and is authorised to conclude the transaction. For example, when a merchant swipes a customer's credit card, the credit card terminal connects to the merchant's acquirer, or credit card processor, which verifies that the customer's account is valid and that sufficient funds are available
25 to cover the transaction's cost. However, this process does not provide any form of verification that the individual making the transaction is indeed authorised to do so.

Although, a merchant may compare a signature on the credit card to the signature of the customer, such methods of verifying whether or not the
30 transaction is fraudulent are far from foolproof. Furthermore, the account holder and credit card provider are relying on the merchant to deny transactions that appear to be fraudulent and unauthorised.

This issue is particularly pronounced with transactions conducted in the online environment or over the telephone, where the merchant is unable to verify the customer's signature and therefore determine whether or not the transaction is fraudulent.

5 One method of overcoming such issues is to require the purchaser to provide a Card Verification Value Code (CVV), which is not part of the card number itself, and is also known as CVV2, CVC2, and CID. The CVV is an authentication procedure established by credit card companies to reduce fraud for internet and telephone transactions. It consists of requiring a card holder to
10 provide the CVV number at transaction time to verify that the card is on hand. While the CVV code helps ascertain that the customer placing the order actually possesses the credit/debit card and that the card account is legitimate, this authentication procedure is ineffective when the card itself has been misappropriated or in scenarios where there has been unauthorised access to the
15 financial records of the account holder.

Similarly, in current systems where the customer is required to provide a password or pin number before a transaction is authorised, unauthorised access to the account holder's records is likely to provide the information required to fraudulently authorise transactions.

20 Accordingly, it is an object of the invention to provide a system for authorising transactions which seeks to alleviate the problems of prior art systems.

It will be clearly understood that, if a prior art publication or systems are referred to herein; this reference does not constitute an admission that the
25 publication or system forms part of the common general knowledge in the art in Australia or in any other country.

SUMMARY OF THE INVENTION

Broadly, the invention allows transactions, such as credit card payments, online banking funds transfers, or others, to be securely authorised by a
30 customer, preferably before the transaction is concluded by the relevant institution. In one form, such authorisation occurs when the customer, prompted by an interactive voice response (IVR) system for example, provides one or more unique identifiers to validate his or her identity and authenticate the transaction.

Alternatively, the customer may indicate that the transaction is fraudulent which is in turn communicated to the relevant institution so that appropriate actions may be taken. The information maintained by the authorisation system is separated from the account and customer records of the financial institution in order to

- 5 maximise security in the authorisation process and mitigate the risk of fraudulent authentication of transactions that may arise as a result of unauthorised access to the stored information.

In one aspect, the invention provides a transaction authorisation system for allowing a customer to authorise transactions relating to at least one customer
10 account associated with an institution, the system including:

data storage means for enabling access to

- (a) identification data associated with the customer;
- (b) identification data associated with a remote communication
device (RCD) of the customer; and
- 15 (c) security identifier data associating the at least one customer account with either one or both of (a) and (b);

a first communication means for enabling communication with the customer via the RCD to authorise a transaction on the at least one customer account;

- 20 a data processing architecture including data processing means to identify the customer using (a), identify the RCD using (b) and determine if the transaction is authorised by the customer; and

a second communication means for receiving an authorisation request in relation to the transaction and providing an indication to the institution of whether
25 or not the transaction is authorised by the customer, wherein the authorisation request received and the indication provided to the institution are referenced to the security identifier data.

In another aspect, the present invention provides a method for allowing a customer to authorise transactions relating to at least one customer account held
30 at an institution, the method including the steps of:

- a) an authorisation server receiving an authorisation request from the institution in relation to a transaction on the at least one customer account;

- b) the authorisation server communicating with the customer via a remote communication device (RCD) of the customer to authorise the transaction;
 - c) the authorisation server identifying the customer using identification data associated with the customer to which the authorisation server has access;
 - d) the authorisation server identifying the RCD using stored identification data associated with the RCD to which the authorisation server has access;
 - e) the authorisation server determining if the transaction is authorised by the customer;
 - f) the authorisation server communicating an indication to the institution of whether or not the transaction is authorised by the customer
- wherein the authorisation request received by the authorisation server and the indication provided to the institution are referenced by the institution and the authentication server to security identifier data for associating the at least one customer account with one or both of the stored identification data associated with the customer and the stored identification data associated with the RCD.
- In one form, the invention resides in a remote payment system allowing a customer to transact payments for goods and services remotely in a secure manner with members of the system, the system including:
- i) data storage means containing updateable data relating to each of a plurality of customers and each of a plurality of members of the system, wherein each customer has at least one associated registry profile with a related monetary reservoir;
 - ii) a data processing architecture including data processing means and a clearing house system for settling indebtedness between members and customers of the system,
 - iii) communications means associated with the data processing architecture for communicating with the customers via a remote communications device (RCD) of each of the customers,

the system being arranged for one or more of said customers to transact payments for goods or services pursuant to a payment request made by one or more of the members, the payment request triggering a communications event from the communications means to the RCD of the relevant customer for the purpose of validating the customer's identity and access to the respective registry profile, and the system being further arranged so as to validate the customer's identity and once such has taken place, allowing the customer to transact payments provided a positive balance remains in the monetary reservoir.

In a second form, the invention resides in a remote payment method allowing a customer to transact payments for goods and services remotely in a secure manner with members of a remote payment system, the system including:

- i) data storage means for containing updateable data relating to each of a plurality of customers, and each of a plurality of members of the system, wherein each customer has at least one associated registry profile with a related monetary reservoir;
- ii) data processing architecture including data processing means and a clearing house system for settling indebtedness between members and customers of the system,
- iii) communications means associated with the data processing architecture for communicating with the customers via a remote communications device (RCD) of each of the customers,

wherein the customer uses the system to transact payments for goods or services pursuant to a payment request made by one or more the members, the payment request triggering a communications event from the at least one communications means to the RCD of the relevant customer for the purpose of validating the customer's identity and access to the respective registry profile, and once the customer's identity has been validated, the customer being allowed to transact payments provided a positive balance remains in the monetary reservoir.

The term transaction is intended to broadly cover various actions which may be performed on an account, such as payment requests, order requests, share transfers, funds transfers, proof of identity requests, requests to release information, or a combination of these actions. Such actions may also be initiated in variety of ways, for example, a payment request may originate from a credit

card transaction at a physical store, a purchase on an ecommerce website (click-to-buy), or a remote payment system which uses a customer's mobile phone to pay for goods and services such as text-to-buy or talk-to-buy systems.

5 The term customer is intended to be understood to broadly include not just customers of financial institutions, but also, any persons having an account with an institution for example, employees, suppliers, or citizens relating to a government agency.

10 The invention advantageously provides the customer with an opportunity, preferably using at least one means of communication that is 'off line' and therefore less susceptible to security breaches, to authorise or flag a transaction before it is approved by the bank or credit card issuer, and funds are transferred to the merchant.

15 Although it is usually desirable for the authorisation of a transaction to take place close to the end of the transaction process, it is to be appreciated that the authorisation of the transaction may take place at any point during the transaction process. For example, it is envisioned that the authorisation of the transaction may occur even before a request for funds is made by the merchant. This is particularly advantageous in online environments where processing times of transactions are usually required to fall within specified constraints.

20 It is also envisioned that the invention can be applied in situations where a pre-approval authorisation is provided without first contacting the customer, allowing the transaction to proceed without delay. However, if the customer, once contacted in regards to the transaction, fails to authorise the transaction or flags the transaction as being unauthorised, the pre-authorisation is immediately
25 revoked and if funds have already been transferred, they are also retrieved.

30 Use of a secure identifier such as a PIN which is memorised by the customer or biometric data (eg voice print, finger print, retina scan, behaviometric etc) means that the transaction is only authorised once the identity of the customer, using information which is not normally available to a fraudulent person, is verified. A further advantage is provided by the fact that the customer's verification and contact details in the system are maintained in a separate data store to the customer's bank details with only a single security identifier (known only to the bank's system and the authorisation system) linking the separated

data stores. Such a setup provides increased security as unauthorised access to any one of the data stores on its own will not provide information adequate to circumvent the authorisation system and conduct fraudulent transactions.

The system of the present invention is particularly useful for customers
5 who do not have access to conventional banking facilities or those who simply want a more convenient and secure manner in which to authorise payments for goods and services, or other transactions, in a secure manner. Fees may be levied by the system administrator for transactions effected using the system, and which may be flat fees or percentages of transaction amounts, or a combination
10 thereof.

The remote communications device (RCD) may be any device capable of communication and is not limited to one-way or two-way communications devices. Examples of preferred forms of RCDs include the customer's fixed or mobile telephone, a personal computing device (whether mobile or fixed) or a
15 facsimile or pager of the customer. All of these devices and others which are not listed but are included as a RCD can generally have a software component.

Any RCD(s) which a customer wishes to use with the system should be registered with the system and accordingly, information identifying the RCD (which is normally unique to that RCD) is recorded for use in the identification
20 process.

The customer may designate which RCD or group of RCDs they wish to use for contact with the system and if a group is designated, for example, for multifactor authentication (discussed below), the customer may additionally designate which RCD is to perform in which manner within the multifactor
25 identification process.

Authorisation for a particular transaction will be dependant upon the validation of the customer's identity which will typically be required before authorisation for the transaction is given. The system sets the verification of the customer's identity as a pre-authorisation condition, and the transaction will
30 preferably be blocked before authorisation if the condition is not satisfied. In other words, the transaction will be declined if the identity of the customer cannot be established by the system. An alert may be sent to the system administrator,

notifying the system administrator of the failure to verify the identity of the customer, allowing steps to refuse or block the transaction request to be taken.

Usually, authorisation for transactions is generally given by financial institutions dependant upon the satisfaction of the identification parameter and/or
5 other parameters as long as that the transaction amount does not exceed the credit limit and/or the membership is still valid and the like. The system of the present invention may operate as a further part of this authorisation process. The system may be associated with the data feed used during the authorisation process and the satisfaction or contravention of the identification criteria
10 communicated to the system administrator may be a further parameter which may be required before authorisation is given by the financial institution.

In the context of a common credit card transaction, for example, the customer, who is typically the owner of the card, uses the card to make a purchase from a merchant, which is the business accepting credit card payments
15 for products or services sold to the customer. The merchant generally collects the card information, by swiping the card through a reader or similar machine if it is a physical store, or otherwise via the Internet or telephone.

As the merchant will wish to verify, for example, that the card is valid and the credit card customer has sufficient credit to cover the purchase, electronic
20 verification is conducted using a credit card payment terminal, Point of Sale (POS) system or like with a communications link to the merchant's acquiring bank. Data from the card is obtained from a magnetic stripe or chip on the card, a chip on a customer device, or is provided by the customer in an online form or verbally over the telephone.

25 The acquirer, ie the financial institution or other organisation that provides card processing services to the merchant, contacts the card issuer via the card association, ie a network such as VISA or MasterCard (and others) that acts as a gateway between the acquirer and issuer for authorising and funding transactions.

30 The issuer, preferably before authorising and funding the transaction, forwards the request to the system of the present invention for authorisation from the customer.

It is to be appreciated, that such customer authorisation requests are not limited to payment systems involving credit cards, but may be equally applied to financial transaction systems involving debit cards, funds transfers between accounts, share purchases, etc, or for example, when accessing secure systems across a network and a request for the purpose of authorising the remote system access is issued.

A complete remote payment system in which the customer authorisation request is received and processed directly by the system is also envisioned and described in detail below.

10 Importantly, regardless of the manner in which the contact for payment is made using the system, the substantive portions of the authentication and validation processes will preferably take place beginning with the system contacting the designated RCD of the customer and preferably using an interactive voice response (IVR) system or similar system to verify the identity of the customer. The authentication process may include one or more factors and methods of contact with the customer and authentication including, but not limited to, IVR systems, biometric information relating to the customer such as voice recognition in particular, code entry from one or more sources along one or more communications channels, generated codes, Radio Frequency ID (RFID), one time only codes or the like.

20 Two-factor authentication may be used in an attempt to overcome newer forms of fraud, as has using two different communications paths. For example, the system may communicate a challenge to the customer cell phone via SMS and expect a specified reply. If it is assumed that all of the bank's customers have cell phones then this results in a two-factor authentication process without extra hardware. Multifactor authentication will typically involve the use of more than one communications channel or sessions wherein a challenge can be issued on a first channel and, the customer response or second authentication piece is communicated over a different communications channel or different communications session than the first, requiring the customer to have access to both in order to comply, making eavesdropping much more difficult. The communications channels will typically be directed to a particular RCD which itself will normally have unique identifying information which will also be required to

match or correlate the customer verification information stored by the system before authentication is granted.

The system uses the authentication request as the basis for contacting the customer via the customer's at least one RCD using a data entry prompt. The data entry prompt may be a message requesting the input of particular private identification (private ID) information such as a code or other verification data, an original entry of which is created by the customer or generated when the customer's account are initially linked to the system and which may be changed as required.

Information relating to one or more private IDs, and one or more RCDs of the customer are stored by the system, but kept separate from the account information of the customer which is maintained by the systems of the relevant institution. The information relating to a particular customer in the system and the systems of the financial institution using a unique security identifier (Security ID) which does not necessarily relate to an identifying characteristic of the customer or the customer's RCD, and not even required to be provided to the customer.

The system compares the private ID information received from the customer, or aspects of the information provided, pursuant to the data entry prompt, to the private identification data maintained by the system for verification purposes. Advantageously, the respective private identification data from the customer and that stored by the system are secured with encryption mechanism such as hashing.

The most preferred form of contact with the customer for authentication purposes is the system using an interactive voice response (IVR) component, which is a computerised system that allows a person, typically a telephone caller, to select an option from a voice menu and otherwise interface with a computer system. Generally the system plays pre-recorded voice prompts to which the person presses a number on a telephone keypad to select the option chosen, or speaks simple answers such as "yes", "no", or numbers in answer to the voice prompts.

The latest systems use natural language speech recognition to interpret the questions that the person wants answered. The newest trend is Guided Speech IVR which integrates live human agents into the design and workflow of

the application to help the speech recognition with human context. IVR developed as a telephony system but similar systems are now available that function on non-telephony systems and any functionally equivalent system or combinations of systems can be used.

5 Typically, an IVR component is included in the at least one communication means and upon the data processing architecture receiving an authentication prompt, the IVR component will typically contact the customer using their preferred remote communications device (RCD). The RCD is likely to be a mobile telephone or similar and the IVR system can then guide the customer through the
10 entry of their identification information to be used in the authentication process. Importantly, the communication means of the system will also typically have the ability to determine the identification characteristics of the particular remote communications means used, such as SIM card numbers or IP addresses, or digital certificates and the like in order to identify the customer according to a
15 multifactor authentication process.

If the verification data entered, matches or correlates to the verification data on file, then the customer is considered to be validated for authorising the transaction. If the verification data entered, does not match or correlate to the verification data on file, then the customer is considered not to be validated and is
20 rejected from the system.

The invalid entry of verification data may also flag a follow up from the system administrator. Preferably, once invalid verification data is entered a predetermined number of times, which may be at least once but preferably no more than three times, that customer may be locked out of the system for a
25 period of time. The lockout may be active on the customer account(s) or may be limited to lockout of access to the system from the particular remote communications means used by the customer as determined using the identification characteristics of the particular remote communications means used.

30 Once authentication is granted or declined, an appropriate indication is provided to the relevant financial institution(s) and a suitable message advising the customer of the outcome of the authentication process is preferably

generated by the data processing architecture and forwarded to the customer's preferred RCD.

BRIEF DESCRIPTION OF THE INVENTION

Preferred embodiments of the present invention will now be described with
5 reference to the accompanying drawings, in which:

Fig. 1 is a context diagram providing an overview of a preferred embodiment of the invention;

Fig. 2 is a flowchart outlining the setup process of a preferred embodiment of the invention;

10 Fig. 3 is a flowchart outlining the authorisation process of a preferred embodiment of the invention;

Fig. 4 is a flowchart outlining the device changing process of a preferred embodiment of the invention;

15 Fig. 5 is a flowchart outlining the customer identifier changing process of a preferred embodiment of the invention;

Figure 6 is a context diagram providing an overview of a remote payment system incorporating a preferred embodiment of the present invention;

Figure 7 is a flowchart outlining a customer registration process of a remote payment system incorporating a preferred embodiment of the present
20 invention;

Figure 8 is a flowchart outlining a website registration process of a remote payment system incorporating a preferred embodiment of the present invention;

Figure 9 is a flowchart outlining a customer authentication process of a remote payment system incorporating a preferred embodiment of the present
25 invention;

Figure 10 is a flowchart outlining a first deposit process of a remote payment system incorporating a preferred embodiment of the present invention;

Figure 11 is a flowchart outlining a purchase process of a remote payment system incorporating a preferred embodiment of the present invention;

30 Figure 12 is a flowchart outlining a funds transfer process of a remote payment system incorporating a preferred embodiment of the present invention;
and

Figure 13 is a flowchart outlining a balance enquiry process of a remote payment system incorporating a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENT

The present invention is not specific to any particular hardware or software implementation, and is at a conceptual level above specifics of implementation. It is to be understood that various other embodiments and variations of the invention may be produced without departing from the spirit or scope of the invention. The following is provided to assist in understanding the practical implementation of particular embodiments of the invention.

10 The authorisation system 20, as shown in Fig. 1, includes a data processing means, ie server 22, with communication means 26 which communicates with an institution system 10 of an institution 50 and a customer device 30 of a customer 40. The customer 40 is generally a customer of the institution 50, but may be an employee, supplier, citizen relating to a government agency or similar. In various circumstances, therefore, the customer 40 may be identified by the institution system 10 using any form of public identification data (Public ID), such as an account number, credit/debit or other card number, employee number, login name, password, or other suitable identifier. In some instances, a combination of these identifiers may be used as a Public ID.

20 Identification information relating to, for example, the institution 50, the customer device 30 and the customer 40, are securely stored in database 24 of the authorisation system 20. The database 24 may take any one of several forms, for example, a single central database, a distributed database or a number of secure databases.

25 It will be appreciated that while the authorisation system 20 is discussed in the context of a financial institution, such as a credit card issuer, the institution 50 may be any organisation requiring secure authorisation of a transaction. Examples of such institutions include an employer, bank, government agency, share broker or any other entity which is seeking secure identification or authorisation.

30 It will also be appreciated that while the authorisation system 20 is discussed in the context of a financial transaction, the transaction may take other suitable forms, such as for example, a request for identification of the customer

40. Examples of transactions requiring authorisation by the authorisation system 20 include an online or over the counter financial transaction, a request to approve a share purchase or sale, or a request for identification which may be required for the customer 40 to enter a building, open an account, or deal with an institution or government agency.

In one form, the authorisation system 20 and the institution system 10 may be hosted in the same secure environment to minimise the chances of communications between them being intercepted by an unauthorised party or if the authorisation system 20 is being incorporated by the institution 50 into their own secure processing layer.

However, where the authorisation system 20 and the institution system 10 are hosted in separate physical environments, communications between them should preferably be facilitated via a secure link such as a direct connection, preferably utilising 'off-net' (ie non Internet or web based) technologies such as a frame or a secure point to point connection. Where the authorisation system 20 and the institution system 10 communicate via the use of 'on-net' technologies, strong authentication and encryption methods, such as VPN tunnelling with challenge authentication or similar technology such as Client/Server certificates, should preferably be used. In such cases, it is preferred that the data communicated across the connection is encrypted with a minimum encryption of 128 bit. Additional security may be provided by authenticating the data packages using a HMAC (Keyed-hash Message Authentication Code) algorithm in which the institution system 10 is provided with a secret key and all information sent by the institution system 10, is hashed against the key to authenticate the data. Furthermore, additional security layers for transmitted data can be also be added if required, such as for example encryption hardware.

It is preferred that changes to the authorisation system 20 should be automatically logged and maintained within a secure audit trail which cannot be changed even at a privileged or administration access level, and should be available in a report format.

Whether the authorisation system 20 and the institution system 10 are securely co-located or securely connected remotely, a unique security identifier, hereinafter referred to as the Security ID is used to correlate the information

relating to the customer 40 in both the authorisation system 20 and the institution system 10, once the setup procedure, as shown in Fig. 2, has been completed for a new user. The Security ID negates the need to constantly transmit identification information about the customer 40 or customer device 30 (discussed below)

5 which may be more easily recognised by third parties.

In this way the account information of the customer 40, stored in the institution system 10, is kept substantially independent from the authorisation system 20.

10 In other words, the use of the Security ID ensures that if either the authorisation system 20 and the institution system 10 is successfully attacked and the records of the customer 40 are accessed by an unauthorised party, there is minimal opportunity for the attacker to obtain the full set of information, and more specifically, identifiers required to complete a transaction, which are discussed in further detail below.

15 In order to maximise the security of the communications and information stored within the database 24, it is preferred that the Security ID is not visible to the customer 40, or the call centres for the institution 50 or the authorisation system 20.

20 So as to facilitate correlation of the transmitted data with the data stored by the institution system 10, the Security ID may be correlated in a secure manner to an existing unique identifier used by the institution system 10, such as for example, an account number of the customer 40. Similarly, the Security ID may be correlated in a secure manner to a unique identifier within the authorisation system 20, which is visible to call centres, etc.

25 During the customer setup process in the system 20, the Institution 50 passes the Device ID to the system 20. The system 20 contacts the customer 40 (via the device 30) 'off-net'. At this point the customer 40 is able to follow the required steps to establish at least one Customer ID. The system 20 then passes back to the Institution 30 the Device ID, and a new unique security identifier (Security ID). Thereafter, the only identifier relating to the customer 40 and/or the device 30, which passes between the Institution 50 and the system 20, is the Security ID.

Therefore, for a fraudulent user seeking to gain unauthorised access to a complete dataset, would need a customer's 40 Public ID, the Device ID and the Customer ID. To gain all this information, they would need to attack and gain unauthorised access to the Institution system 10, follow a transaction to the
5 authorisation system 20 and attack the link between the system 20 and the customer device 30. Thereby, in an example set in the banking context, the unauthorised user would need to attack and gain unauthorised access to the bank, the authorisation system 20 and the mobile phone network on which the device 30 is connected.

10 In a typical financial transaction situation, as shown in Fig. 3, the merchant or similar organisation will request the institution 50 for authorisation of the transaction. In some cases, where such authorisation is not requested by the merchant or where the transactions are internal to the institution 50, the institution 50 may itself request authorisation of the transaction. It is at this point that the
15 institution system 10 sends an authorisation request 15 to the authorisation system 20, which in turn contacts the customer 40 for authorisation of the transaction.

Where the authorisation system 20 is connected to a number of institutions and/or institution systems, the authorisation request 15 may include a unique
20 identifier to identify the institution 50, hereinafter referred to as the Institution ID, which is communicated to the authorisation system 20 with the authorisation request 15. In situations, for example, where the institution 50 hosts the authorisation system 20, the Institution ID may not be necessary. Also, it will be appreciated that the Institution ID may be in different forms such as the internet
25 protocol (IP) or media access control (MAC) address of a server, or a combination of identifying numbers and/or letters.

The customer 40 is contacted by the authorisation system 20 on the customer device 30. The customer device 30 may be a handheld device such as a mobile phone or personal data assistant (PDA), or a portable computer such as
30 a laptop. It is intended that the customer 40 is contacted on a portable device carried with the customer 40 as this will ensure that transactions can be authorised as required and without unnecessary delay.

It is preferred that the communication with the customer device 30 is conducted over an off-net communication network (ie non-internet or web based technology), particularly in situations where the transaction itself has been conducted over the internet or web. In this way, even if the transaction session is compromised, the authorisation process remains secure as it is carried out over a different communication network and is therefore unlikely to be also compromised. Also, where a communication network, which is the same as the one over which the transaction is conducted, is used, the authorisation process may be conducted over a separate session to the transaction session, or may itself be affected over more than communication session.

In order to establish a secure communication session between the authorisation system 20 and customer device 30, suitable security measures are adopted. The exact nature of these security measures will of course be determined by the type of device, the connection method used and the network type.

For example, in the case of a GSM mobile phone, a 128-bit Ki within the mobile's SIM is used to uniquely identify the device to the network. A 128-bit random challenge (RAND) is provided by the network with the device then providing a 32-bit response (SRES). A 64-bit ciphering key (Kc) creates a basis for encryption during the session. Underlying algorithms include A3 (authentication), A5 (Encryption) and A8 (Key Generation), and other security layers as required.

In the case of a CDMA device, the electronic serial number and an A-key programmed into the phone are used to uniquely identify the device to the network. A random binary number (RANDSSD) is generated by the network with the device responding with a required 128-bit sub key called a Shared Secret Data (SSD). Part of the SSD is used for authentication, and part for encryption, and underlying algorithms may include standard CAVE, CMEA, E-CMEA, or ORYX in the case of data. In addition to the foregoing, CDMA2000 and WCDMA can be used to apply additional layers of security such as SHA-1, AES, the Kasumi and Rijndael algorithms and the AKA protocol.

In the event that Wi-Fi (802.11 base technology), Bluetooth® and other Near Field Communication technologies, as well as long range communication

technologies, are used to communicate with the customer device 30, it is preferable to implement strong security practices available with such technologies.

In order to identify the customer device 30 to the authorisation system 20, a unique device identifier, hereinafter referred to as the Device ID, of the customer device 30 may be compared to the Device ID provided by the customer device 30. Examples of such identifiers include a phone number, an International Mobile Equipment Identity (IMEI) which is a number unique to every GSM and UMTS mobile phone, IP or MAC address, or any other form or combination which uniquely identifies the customer device 30 to the authorisation system 20.

It will be appreciated that in some cases, for example, where the Device ID includes a phone number, the information therein will be used to also initiate a communication with the device 30. However, where the Device ID consists only of device identifiers such as a MAC address, which in themselves are not able to be utilised to initiate a communication with the device 30, additional contact information for communicating with the device 30 may also be stored by the system 20.

The authorisation system 20 provides a procedure, as shown in Fig. 4, for changing the Device ID stored in database 24, for example, if the customer 40 obtains a new customer device 30.

In order to authorise the transactions, the customer 40 is prompted by the authorisation system 20 to provide at least one unique customer identifier, hereinafter referred to as the Customer ID, which is used to ensure it is the actual customer approving the transaction, and not another person who simply may have access to the customer device 30. Ideally, the Device ID and the Customer ID are separately secured and may undergo encryption processes such as hashing during storage and/or communication.

The Customer ID may be a personal identification number (PIN) or password/pass-phrase which is known to the customer 40, a biometric identifier such as a voice print, a secret word, a fingerprint, or any other form of identifier which would usually only be known to, or accessible by, the customer 40.

In a preferred form, an interactive voice response (IVR) system, ie IVR system 28, may be used to both prompt the customer 30 for the Customer ID and

subsequently receive the Customer ID. An IVR is a computerised system that allows the customer 40 to select options from a voice menu and otherwise interact with the authorisation system 20. Generally the IVR system 28 plays a pre-recorded voice prompt and the customer 40 presses a number on a telephone keypad to select an option and/or speaks an answer, such as the Customer ID, which is recognized by the IVR system 28.

For example, a Customer ID which includes a 4 (or 6) digit PIN, is not known or stored by authorisation system 20 in a digitised usable form. When the IVR system 28 receives the PIN via DTMF within the session associated with the call, it is encrypted in the session using MD5, and it is only this hash encrypted MD5 string, which is associated with the PIN, that is communicated back to the authorisation system 20 for validation or storage. This procedure ensures that in the unlikely event that the authorisation system 20 is attacked, and the attacker is able to break the encryption that relates the Customer ID to the Device ID, they would not be able to simulate an authorisation call in an attempt to obtain the PIN in usable form for an IVR system unless the MD5 encryption is reversed. Furthermore, additional security layers for data can be also added if required, such as for example encryption hardware.

In an alternate embodiment, which utilises voice biometrics, the Customer ID is formed by the voice print of the customer 40. This voice print may be calculated by asking the customer to repeat a randomly generated word or phrase such as "Yellow" which allows the voice print of the customer 40 to be captured. Preferably, a future authorisation request will request the customer 40 to say a different word or phrase such as "Tuesday" for enhanced security.

In this way, the authorisation system 20 determines the biometric voice print from the response and compares it to the stored data. As another layer of security, the system 20 may also perform a voice to text conversion of the word or phrase and make a further comparison with the stored data to confirm that the word spoken is in fact the one recorded. Thereby, to be broken, a user seeking unauthorised access would require not only a high quality recording of the customer's voice, but would also need to use that recording to say the random word requested.

20

In another alternative embodiment, the system 20 may ask the customer 40 a question to which he or she is likely to know the answer. For example, the system 20 may ask "How much was your last transaction?" or "What is your middle name?". The customer's 40 response is compared not only against the
5 stored voice print data but the accuracy of the response is also determined.

Once the Customer ID is provided by the customer 40, the transaction may be considered by the authorisation system 20 as being authorised. Accordingly, the authorisation system 20 communicates the authorisation of the transaction to the institution system 10, which will in turn allow the institution 50 to
10 take the appropriate actions to conclude the transaction.

The authorisation system 20 provides a procedure, as shown in Fig. 5, for changing the Customer ID stored in database 24, for example, if the customer 40 needs to change his or her password, PIN, etc.

In certain situations, the customer 40 may need to provide a response to
15 the authorisation system 20, either instead of, or in addition to, the Customer ID. This response may be used to communicate a request to cancel the transaction or flag the transaction as fraudulent, for example. In such situations, the authorisation system 20 communicates the fact that the transaction may be fraudulent to the institution system 10, which will in turn allow the institution 50 to
20 take the appropriate actions to cease the transaction and stop the transfer of funds.

It is preferred that the Customer ID and the Device ID are stored by the authorisation system 20 in a manner that separates them, for example by the use of an encrypted algorithm. This is to ensure that in the unlikely event an attack on
25 the authorisation system were successful; the attacker could not correlate the Customer ID and the Device ID, and subsequently emulate authorisation of a fraudulent transaction. In one form the Customer ID is stored separately in a triple fire-walled subset within the authorisation system 20 environment.

It is also preferable that the Customer ID is not stored or copied elsewhere
30 during the transaction authorisation process. This may require the facilitation of a pass-through in the IVR system 28 as opposed to a store and validation method.

According to a particularly preferred embodiment, a remote payment system 100 incorporating the authorisation system 20 is provided.

The functionality and use of one implementation of the system 100 is illustrated in Figures 6 to 13. The remote payment system 100 allows a customer 40 to transact payments for goods and services remotely in a secure manner with members 60 of the system 100. The preferred implementation of the system 100, according to which the uses of the system 100 are illustrated in Figures 6 to 13, includes at least one data storage means 70 for containing updateable data relating to each customer 40, and each member 60 of the system 100, wherein each customer 40 has at least one associated registry profile 80 with a related monetary reservoir 90. The system 100 also includes a data processing architecture 110 having at least one data processing means 120 and a clearing house system 125 for settling indebtedness between members 60 and customers 40 of the system 100, at least one communications means 130 associated with the data processing architecture 110 for communicating with a customer 40, and at least one remote communications device 30 held by each customer 40 for communicating with the communication means 130.

The customer 40 uses the system 100 to transact payments 140 for goods or services pursuant to a payment request 150, the payment request 150 triggering a communications event 165 from the at least one communications means 130 to the at least one remote communications device 30 for the purpose of validating the customer's 40 identity and access to the respective registry profile 80, and once the customer's 40 identity has been validated, allowing the customer 40 to transact payments 140 provided a positive balance remains in the monetary reservoir 90.

There will typically be at least two categories of membership of the system, namely business members 60 and customer members 40. There will typically be a plurality of members in each category of membership. Membership of the business member 60 category may be controlled strictly and/or limited by the system administrator 160. Membership of the customer member 40 category may be provided after an application process which may be subject to approval by the administrator 160. Importantly, business members 60 of the system 100 may be customer members 40 of the system 100 as well.

The system administrator 160 will typically offer membership to the business members 60 and the customer members. The membership may require

a subscription. Business members 60 may generally pay an annual subscription fee which will allow them access to the system 100. The business members 60 may be provided with a unique identification number and password for identification purposes. The business members 60 may receive regular bulletins and updates about the system 100, as well as results of data analysis performed on the information relating to the system 100. These bulletins may be prepared by the system administrator 160. Typically, information such as this will relate to the program and its benefits, advertising of the program or the like. The system administrator 160 may compile a database 170 containing the details of the business members 60 and any other information or statistics that the system administrator 160 desires.

The business member 60 may collect and/or update information on the customer members 40 of the program that use the system 100 to pay for goods or services of the business members 60. This information may be communicated to the system administrator 160 and may be stored on the customer database 70.

There may preferably be two portions or sectors of the system. The two portions of the system may preferably be known as the front end and the back end. The front end may preferably comprise a user interface. The user interface allows a subscriber or database administrator to access or connect to the back end of the system 100. The front end or user interface may preferably be located or accessible using an Internet browser or mobile telephone, PDA or other personal device with communications ability. Alternatively the user interface may be located on a computer or server or a network of computers or servers. It may be of any suitable type or configuration.

The back end of the system 100 may preferably include at least one data storage means typically a plurality of databases. At least one of the databases may preferably be a customer database 70, containing information about customers 40 and their associated monetary registry 90, and the second database may preferably be a business member database 170, containing information about business members 60 and their accounts 180. Access to each of the databases via the user interface may preferably be differentiated depending on the access or login details. For example access by a customer 40 may allow only particular or restricted functions to be performed, which may be

restricted in a manner similar to the access granted to customer members 40 but with the same or different functionalities whereas access by the system administrator 160 may grant "superuser" status and allow access to all portions of the system 100 and all functions of the system 100.

5 Typically, a potential member may contact the system administrator 160 in order to subscribe to the system 100. The system administrator may suitably provide the member with a unique username and password to allow access to the system. The member may preferably pay the system administrator 160 a subscription fee in order to access the system 100 for a preset period of time. The
10 username and password may include a Personal Identification Number, an account number, or the username may be linked to identification characteristics of the remote communications means used and the identification characteristics of the particular remote communications means used by the customer 40 may differ according to the type of the device 30 used. For example, computers using hard
15 wired internet connections may use ID means such as Caller Line Identification (CLI) technology, mobile telephony services may allow SIM card identification characteristics to be used and direct internet access to the interface may use the network address or internet protocol address, preferably validated through a service provider as a username.

20 The above discussion is based around a mobile telephony or computing device. The system 100 can also be used over the Internet for example. Upon opening the predetermined web page, the customer 40 may suitably be prompted to enter their username and password in order to access the system 100. The correct entry of a customer 40 username and accompanying password may
25 preferably allow access to the system 100 as a customer 40.

Use of the system 100 by business members 60 may be slightly different to that of customer members 40. Business members 60 will preferably use the system 100 to notify customers 40 of pending payment requests 150 and to monitor their own account 180 balance. The system 100 may also allow a
30 business member 60 to produce accounting statistical records from the system 100 information.

Use of the system 100 by the system administrator 160 may also preferably be accessed through the front end user interface. In a manner similar

to a customer's 40 entry of their username and password, the administrator 160 may also have a username and password, entry of which may suitably allow broader or unrestricted access to the system 100 than that allowed to a customer 40.

5 The correct entry of the administrator 160 username and accompanying password may preferably allow access to the system 100 as the database administrator. The administrator 160 will preferably have the ability to maintain the system 100, including amending the customer registry profiles 80 and virtual wallets 90 to correct errors and also generate reports from the system 100.

10 Customers 40 may have the option to update their identification details or contact details via, for example, a web interface. Upon selecting the option to modify the customer's 40 details, an editable form is preferably displayed allowing the customer 40 to edit their account details. This may allow the modification of the details such as username, password, contact name and address details
15 including telecommunications numbers, e-mail and customer web site address. Change of identification information in this manner will typically trigger the authentication process to be carried out again.

 Specific preferred features of the system 100 are more easily described with respect to use of the system 100 by a customer 40 or business member 60,
20 or by the administrator 160.

 The first step in the system 100 will generally be to establish a new customer 40 registry profile 80. The events which can initiate a New Customer Registration together with a preferred process for dealing with the events are identified in Figure 7. The front end of the system may preferably be reached
25 using an Internet browser to visit a predetermined web site address. This may be performed by either the customer 40 directly using the internet interface or by contacting a customer service officer (CSO) of the system 100 by other means and the CSO using the internet interface to enter the customer 40 details required for initial validation of the customer 40. The preferred implementation of the actual
30 process of New Customer Registration is illustrated in Figure 8.

 Upon selecting the option to enter the customer 40 details, an editable form is preferably displayed allowing the customer 40 (or CSO) to enter (or edit) their subscription details or account details. This may allow the modification of the

details such as username, password, contact name and address details including telecommunications numbers, e-mail and customer 40 web site address. It may also include other background data such as date of birth, referrer and bank details. If any of the identifying information entered is already in use or piece of
5 information are missing, a prompt may be issued to request the information or correction of the information.

Once the customer's 40 identification information has been validated by a preferred primary validation procedure, the information entered may be used to create a customer 40 registry profile 80 and monetary reservoir or "virtual wallet"
10 90.

Funds for use in the system 100 of the present invention are typically transferred into the customer's 40 virtual wallet 90. The transfer of funds may be from a debit account 210 with an established financial service provider 190 such as a bank, building society or other or from a credit facility offered by a provider
15 190. Preferably, at this stage, the preferred source for the transfer may be nominated by the customer 40 but not processed.

This may be followed by a second authentication procedure typically following a secondary vetting procedure by the system administrator 160 as well as a more thorough check of the information provided which may require
20 confirmation from parties independent of the system administrator 160.

Once the customer 40 advises the system 100 of the preferred source for the transfer, the customer 40 may then be asked to follow an authentication procedure to authenticate their identity, validity of access to the system 100 and to the source account 210 for the transfer or similar. A preferred implementation
25 of the authentication process is illustrated in Figure 9.

The authentication procedure may include the data processing architecture 110 creating an authentication prompt and communicating the authentication to the at least one communication means 130 associated with the data processing architecture 110.

30 The validation and authorisation for the payment 200 is performed using the authentication system 20 outlined earlier. Again, once authentication is granted or declined, a suitable message advising the customer 40 of the outcome of the authentication process will preferably be generated by the data processing

architecture 110 and forwarded to the customer's 40 preferred remote communications device 30 via the at least one communication means 130 associated with the data processing architecture 110.

5 If the authentication process is successful, the payment 200 is recorded by the system 100 and the customer's 40 virtual wallet 90 updated to account for the payment 200 and to accurately reflect the funds available to the customer 40 through the system 100.

10 A post-start-up funds transfer to top up their virtual wallet 90 or balance enquiry or other transaction types will also typically be possible. Each transaction will typically be subject to the authentication process including contacting the customer 40 by the system 100 and the request for validating information.

15 Once the customer's 40 identity has been validated, the customer 40 will typically be prompted to transfer start-up funds into their virtual wallet 90 for use under the system 110. In this case, the customer 40 will typically follow a first deposit procedure, a preferred implementation of which is illustrated in Figure 10. The funds transfer may differ depending upon whether the customer 40 is using a debit or a credit facility. If a credit facility is used, the system 100 may function on a real-time basis, drawing down the credit card information and processing the credit card payment on demand whereas if a debit facility is used, the customer
20 40 may transfer funds into their virtual wallet 90 for use immediately or at a later time.

Following the prompt to transfer start-up funds, the system 100 still using the IVR component 28 and generally on the same contact as the authentication contact, will request that the customer 40 designate the amount to be transferred.
25 The system may then process this request with the customer's 40 nominated financial institution 190 and account and issue a successful/unsuccessful notification to the customer 40. The customer 40 contact with the IVR component 28 may be terminated at that stage or the system 100 may question whether any further activity is to be undertaken by the customer 40. If the transfer is
30 successful, the payment 200 is recorded by the system 100 and the customer's 40 virtual wallet 90 updated to account for the payment 200 and to accurately reflect the funds available to the customer 40 through the system 100.

Typically, for balancing the processing load on the system 100, the customer 40 transactions and updates to the respective virtual wallets 90 may be conducted in real-time but the updating of transfer of funds to the business members 60 of the system 100 may occur in lull periods in the system 100. The
5 update of funds transfers to business members 60 may occur in bulk "squirts" wherein a single amount may be transferred to a business member 60 with the appropriate information to identify the customer payers 40. The timing of the lull periods may occur at a particular time each period, typically each day, or the system 100 may be self-monitoring to process transfers to businesses 60 when
10 the processing of customer 40 transfers drops.

Depending upon the outcome of the first deposit procedure, the registry profile 80 and more particularly, the customer's 40 virtual wallet 90 may be "loaded" with an entry indicating the value of funds transferred from the source account 210 into the customer's 40 virtual wallet 90 which can then be used by
15 the customer 40 to make payments 140 to business members 60 of the system 100 at any time.

A preferred implementation of the payment process is illustrated in Figure 11. In order to make a payment 140 using the system, a payment request 150 will typically be generated through an interface to the system 100 by a business
20 member 60 (a "pull" operation), a customer 40 (a "push" operation) or by other means and the payment request 150 will preferably be tagged and associated with a particular customer's 40 registry profile 80. The customer 40 will also be notified of the pending payment request 150 either by the business member 60 directly or by the system 100 itself.

25 Once the payment request 150 has been generated, the customer 40 indicates that payment 140 using the system 100 is to be performed, normally by contact with the communication means 130 associated with the data processing architecture 120. The data processing architecture 120 then typically verifies the details of the payment request 150 and may also verify the customer 40 identity
30 and the availability of funds in the customer virtual wallet 90 and then forwards a prompt to the communications means 130 to contact the customer 40 for the validation or authorisation for the payment 140.

Again, the validation and authorisation for the payment 140 is performed using the authorisation system 20 outlined earlier. Once authentication is granted or declined, a suitable message advising the customer 40 of the outcome of the authentication process will preferably be generated by the data processing architecture 120 and forwarded to the customer's preferred remote communications device 30 via the at least one communication means 130 associated with the data processing architecture 120.

If the authentication process is successful, the payment 140 is recorded by the system 100 and the customer's 40 virtual wallet 90 updated to account for the payment 140 and to accurately reflect the funds available to the customer 40 through the system 100.

A post-start-up funds transfer to top up their virtual wallet 90 (a preferred implementation of this process is illustrated in Figure 12) or balance enquiry (a preferred implementation of this process is illustrated in Figure 13) or other transaction types will also typically be possible. Each transaction will typically be subject to the authentication process using authentication system 20 including contacting the customer by the system 100 and the request for validating information.

In the present specification and claims (if any), the word "comprising" and its derivatives including "comprises" and "comprise" include each of the stated integers but does not exclude the inclusion of one or more further integers.

Reference throughout this specification to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment is included in at least one embodiment of the present invention. Thus, the appearance of the phrases "in one embodiment" or "in an embodiment" in various places throughout this specification are not necessarily all referring to the same embodiment. Furthermore, the particular features, structures, or characteristics may be combined in any suitable manner in one or more combinations.

The foregoing discussion is considered as illustrative only of the principles of the invention. Furthermore, since numerous modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation shown and described, and accordingly, all

suitable modifications and equivalents may be resorted to, falling within the scope of the invention.

CLAIMS:

1. A transaction authorisation system for allowing a customer to authorise transactions relating to at least one customer account associated with an institution, the system including:
- 5 data storage means for enabling access to
- (a) identification data associated with the customer;
- (b) identification data associated with a remote communication device (RCD) of the customer; and
- (c) security identifier data associating the at least one customer
- 10 account with either one or both of (a) and (b);
- a first communication means for enabling communication with the customer via the RCD to authorise a transaction on the at least one customer account;
- a data processing architecture including data processing means to identify
- 15 the customer using (a), identify the RCD using (b) and determine if the transaction is authorised by the customer; and
- a second communication means for receiving an authorisation request in relation to the transaction and providing an indication to the institution of whether or not the transaction is authorised by the customer,
- 20 wherein the authorisation request received and the indication provided to the institution are referenced to the security identifier data.
2. The transaction authorisation system of claim 1, wherein the security identifier data is not communicated to the customer.
3. The transaction authorisation system of claim 2, wherein the security identifier
- 25 data is not the same as, nor derived from, characteristics of or personal information relating to the customer.
4. The transaction authorisation system of any one of claims 1 to 3, wherein the first communication means enables communication with the customer via the RCD utilising a communication medium which is distinct from the communications
- 30 medium utilised to conduct the transaction.

5. The transaction authorisation system of any one of claims 1 to 4, wherein the first communication means enables communication with the customer via the RCD utilising two or more communication sessions.
6. The transaction authorisation system of any one of claims 1 to 5, wherein (a)
- 5 includes one or more of a PIN, a password, pass phrase, or biometric data.
7. The transaction authorisation system of any one of claims 1 to 6, wherein (b) includes one or more of a phone number, an International Mobile Equipment Identity (IMEI), Internet Protocol (IP) address, or Media Access Control (MAC) address.
- 10 8. The transaction authorisation system of any one of claims 1 to 7, wherein the first communication means includes an interactive voice response (IVR) system.
9. The transaction authorisation system of any one of claims 1 to 8, wherein the data storage means further enables access to RCD contact information for use by the first communication means in enabling communication with the customer via
- 15 the RCD.
10. A method for allowing a customer to authorise transactions relating to at least one customer account held at an institution, the method including the steps of:
- a) an authorisation server receiving an authorisation request from the institution in relation to a transaction on the at least one customer
 - 20 account;
 - b) the authorisation server communicating with the customer via a remote communication device (RCD) of the customer to authorise the transaction;
 - c) the authorisation server identifying the customer using identification
 - 25 data associated with the customer to which the authorisation server has access;
 - d) the authorisation server identifying the RCD using stored identification data associated with the RCD to which the authorisation server has access;

- e) the authorisation server determining if the transaction is authorised by the customer;
- f) the authorisation server communicating an indication to the institution of whether or not the transaction is authorised by the customer

5

wherein the authorisation request received by the authorisation server and the indication provided to the institution are referenced by the institution and the authentication server to security identifier data for associating the at least one customer account with one or both of the stored identification data associated with the customer and the stored identification data associated with the RCD.

10

11. The transaction authorisation method of claim 10, wherein the security identifier data is not communicated to the customer.

12. The transaction authorisation method of claim 10 or 11, wherein the security identifier data is not the same as, nor derived from, characteristics of or personal information relating to the customer.

15

13. The transaction authorisation method of any one of claims 10 to 12, wherein the communication with the customer via the RCD utilises a communication medium which is distinct from the communications medium utilised to conduct the transaction.

20

14. The transaction authorisation method of any one of claims 10 to 13, wherein the communication with the customer via the RCD utilises two or more communication sessions.

25

15. The transaction authorisation method of any one of claims 10 to 14, wherein the stored identification data associated with the customer includes one or more of a PIN, a password, pass phrase, or biometric data.

16. The transaction authorisation method of any one of claims 10 to 15, wherein stored identification data associated with the RCD includes one or more of a

phone number, an International Mobile Equipment Identity (IMEI), Internet Protocol (IP) address, or Media Access Control (MAC) address.

17. The transaction authorisation method of any one of claims 10 to 16, wherein the communication with the customer via the RCD includes the use of an
5 interactive voice response (IVR) system.

18. The transaction authorisation method of any one of claims 10 to 17, wherein communication with the customer via the RCD is enabled using stored RCD contact information.

19. A remote payment system allowing a customer to transact payments for
10 goods and services remotely in a secure manner with members of the system, the system including:

- i) data storage means containing updateable data relating to each of a plurality of customers and each of a plurality of members of the system, wherein each customer has at least one associated registry
15 profile with a related monetary reservoir;
- ii) a data processing architecture including data processing means and a clearing house system for settling indebtedness between members and customers of the system,
- 20 iii) communications means associated with the data processing architecture for communicating with the customers via a remote communications device (RCD) of each of the customers,

the system being arranged for one or more of said customers to transact payments for goods or services pursuant to a payment request made by one or more of the members, the payment request triggering a communications event
25 from the communications means to the RCD of the relevant customer for the purpose of validating the customer's identity and access to the respective registry profile, and the system being further arranged so as to validate the customer's identity and once such has taken place, allowing the customer to transact payments provided a positive balance remains in the monetary reservoir.

20. A remote payment method allowing a customer to transact payments for goods and services remotely in a secure manner with members of a remote payment system, the system including:
- 5 i) data storage means for containing updateable data relating to each of a plurality of customers, and each of a plurality of members of the system, wherein each customer has at least one associated registry profile with a related monetary reservoir;
 - 10 ii) data processing architecture including data processing means and a clearing house system for settling indebtedness between members and customers of the system,
 - 15 iii) communications means associated with the data processing architecture for communicating with the customers via a remote communications device (RCD) of each of the customers,
- wherein the customer uses the system to transact payments for goods or
- 15 services pursuant to a payment request made by one or more the members, the payment request triggering a communications event from the at least one communications means to the RCD of the relevant customer for the purpose of validating the customer's identity and access to the respective registry profile, and
- 20 once the customer's identity has been validated, the customer being allowed to transact payments provided a positive balance remains in the monetary reservoir.
21. A remote payment system allowing a customer to transact payments for goods and services remotely in a secure manner with members of the system including a transaction authorisation system according to any one of claims 1 to 9.
- 25 22. A transaction authorisation system according to any one of claims 1 to 9 for use in the context of authenticating credit card transactions.
23. A transaction authorisation system substantially as herein described with reference to any one of the embodiments of the invention illustrated in the accompanying drawings.

24. A method for allowing a customer to authorise transactions substantially as herein described with reference to any one of the embodiments of the invention illustrated in the accompanying drawings.

25. A remote payment system and method substantially as herein described
5 with reference to any one of the embodiments of the invention illustrated in the accompanying drawings.

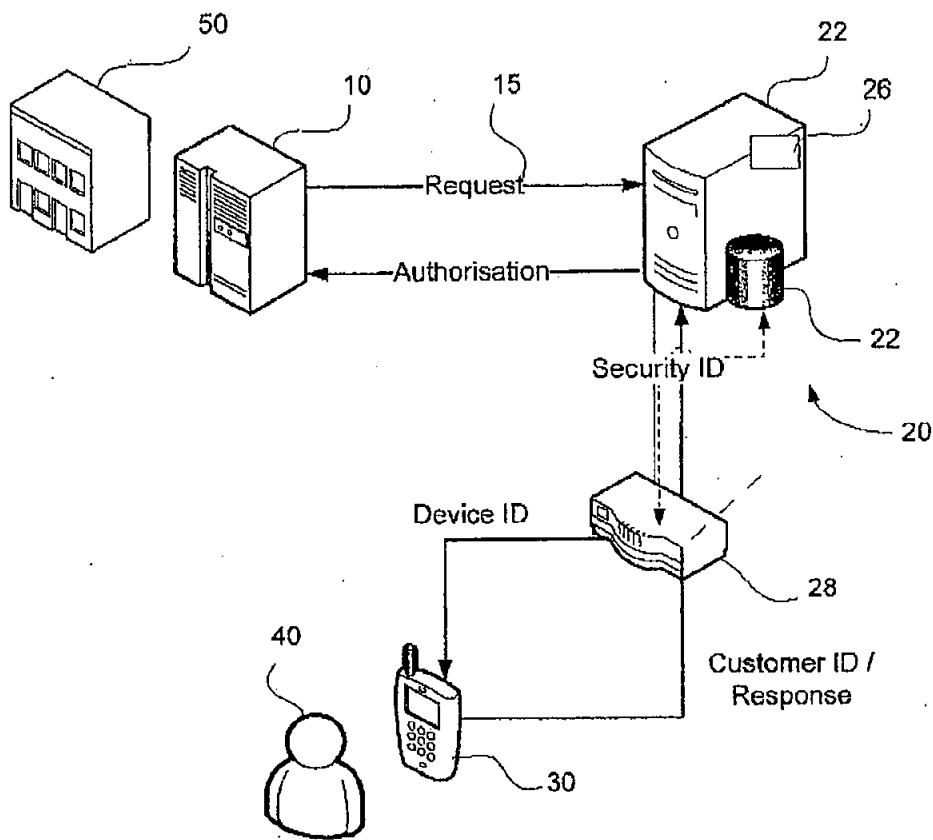


Fig. 1

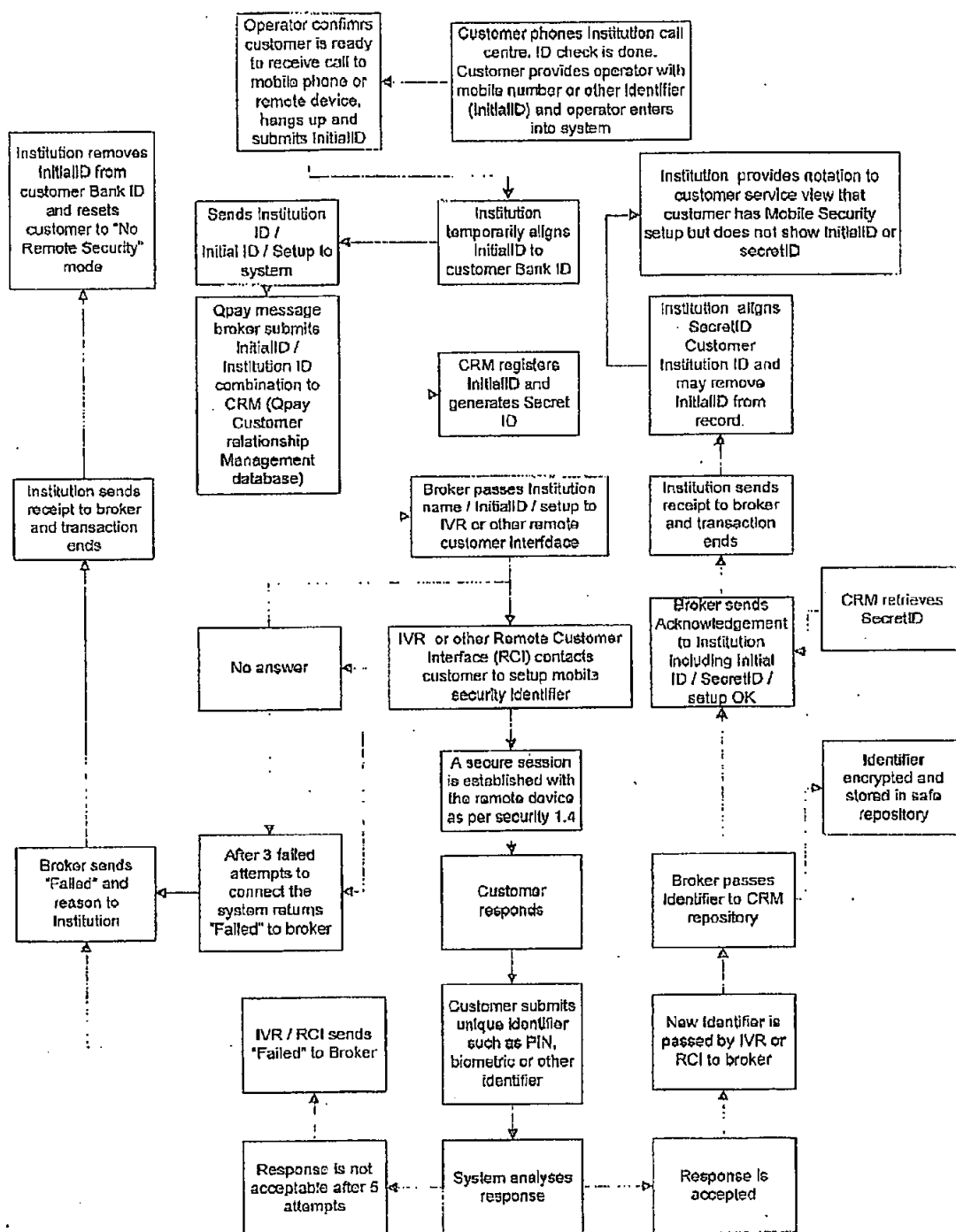


Fig. 2

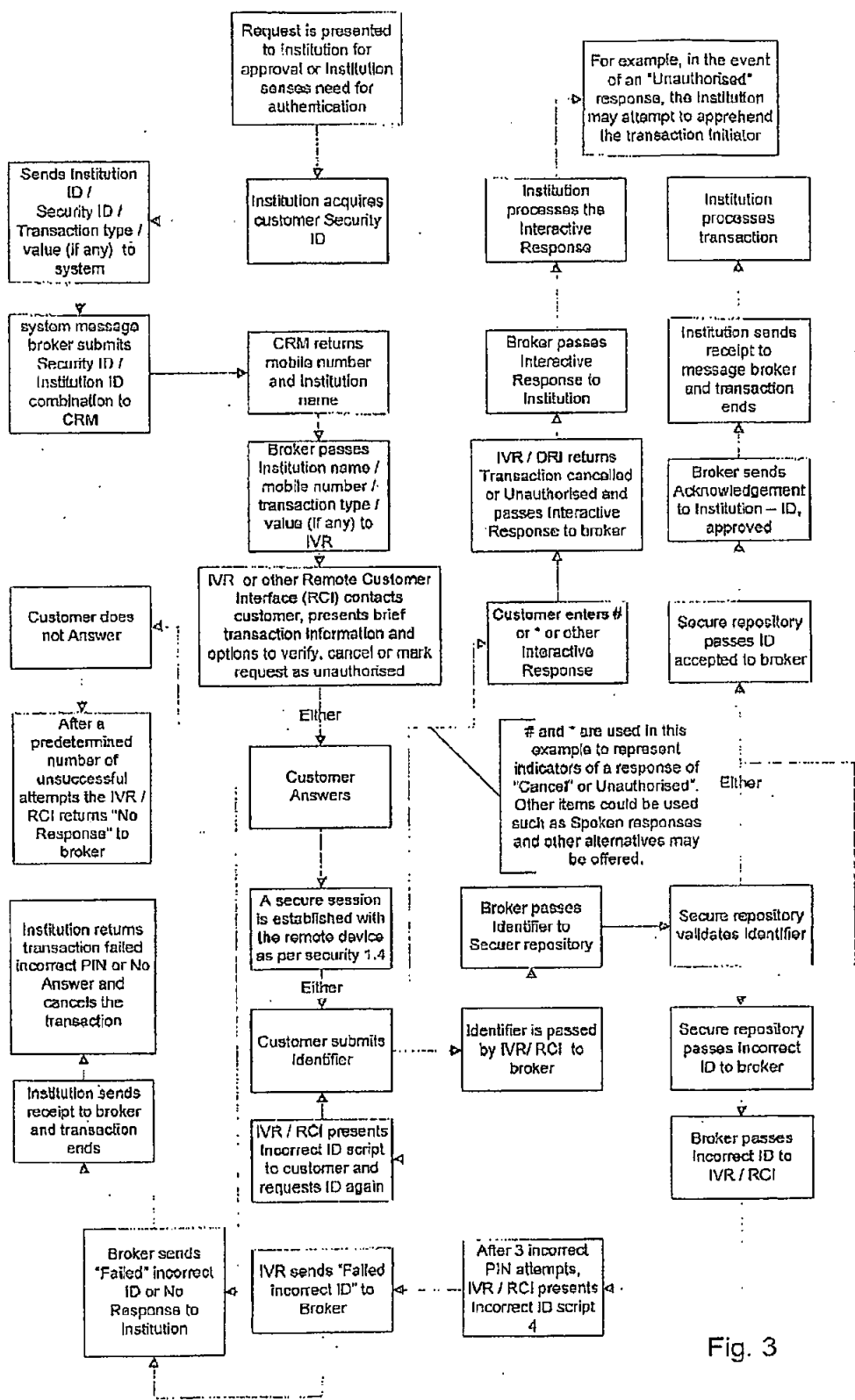


Fig. 3

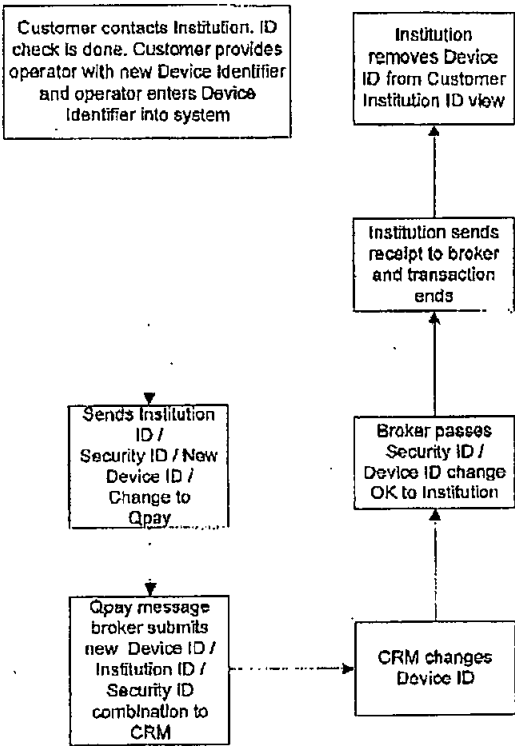


Fig. 4

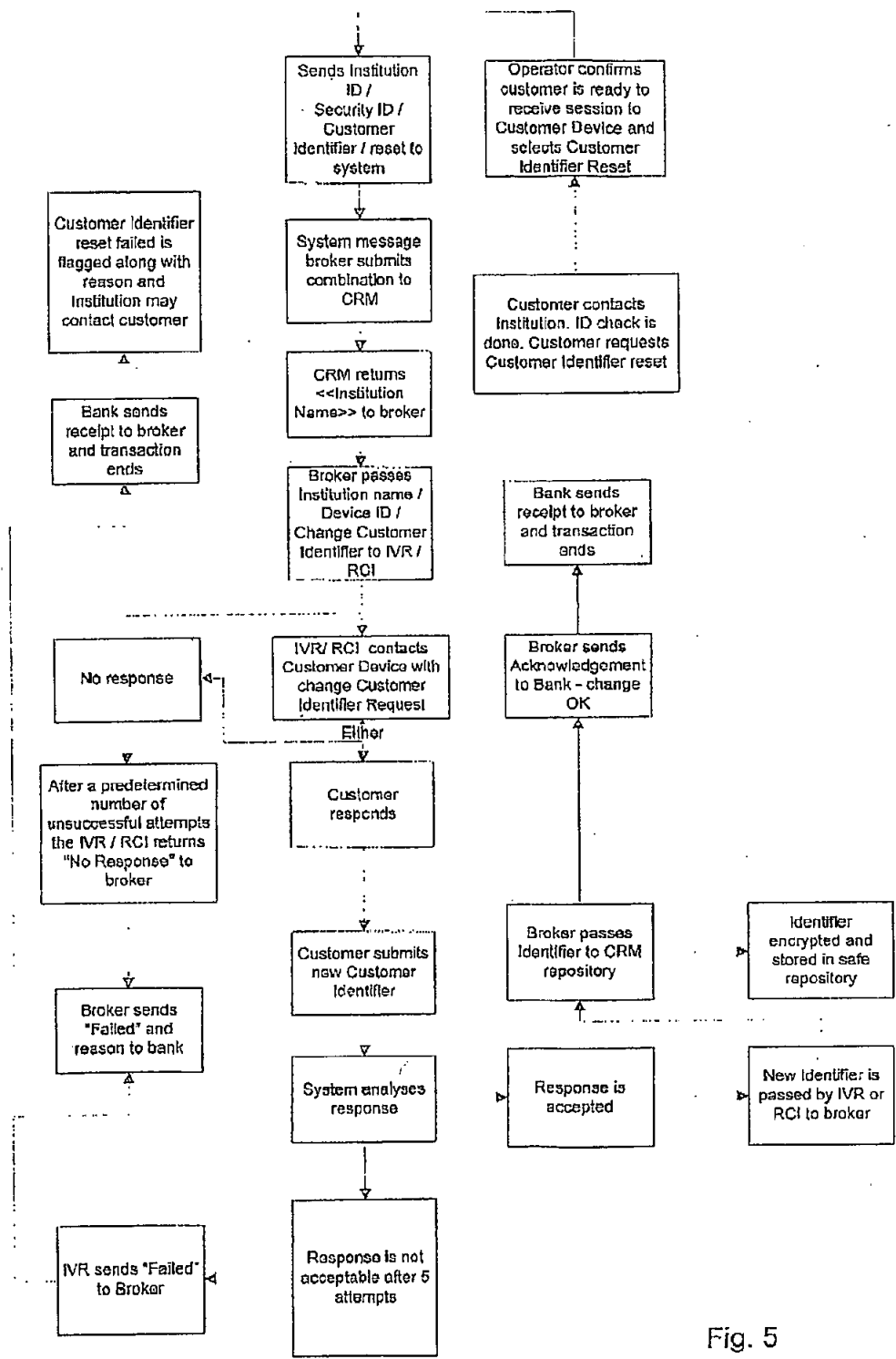


Fig. 5

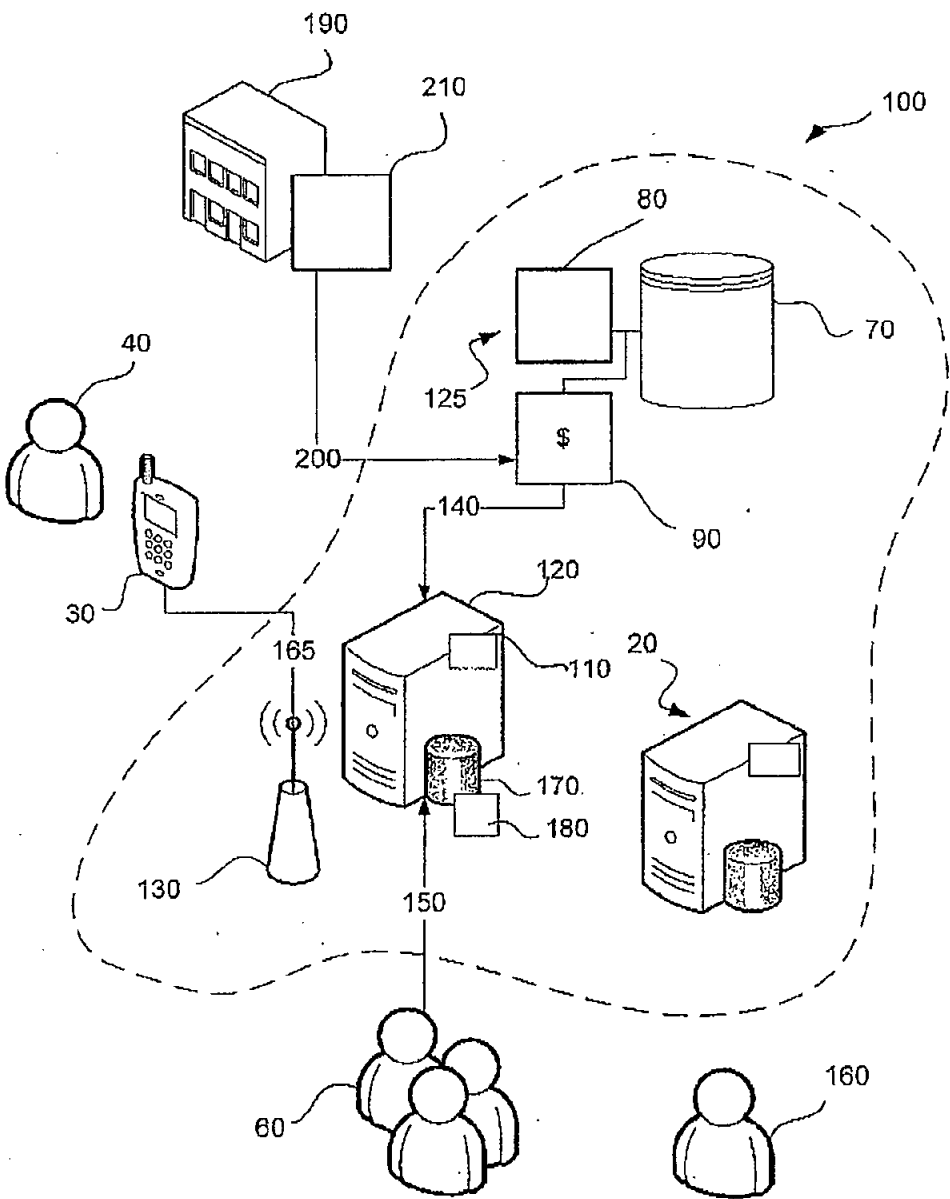


Fig. 6

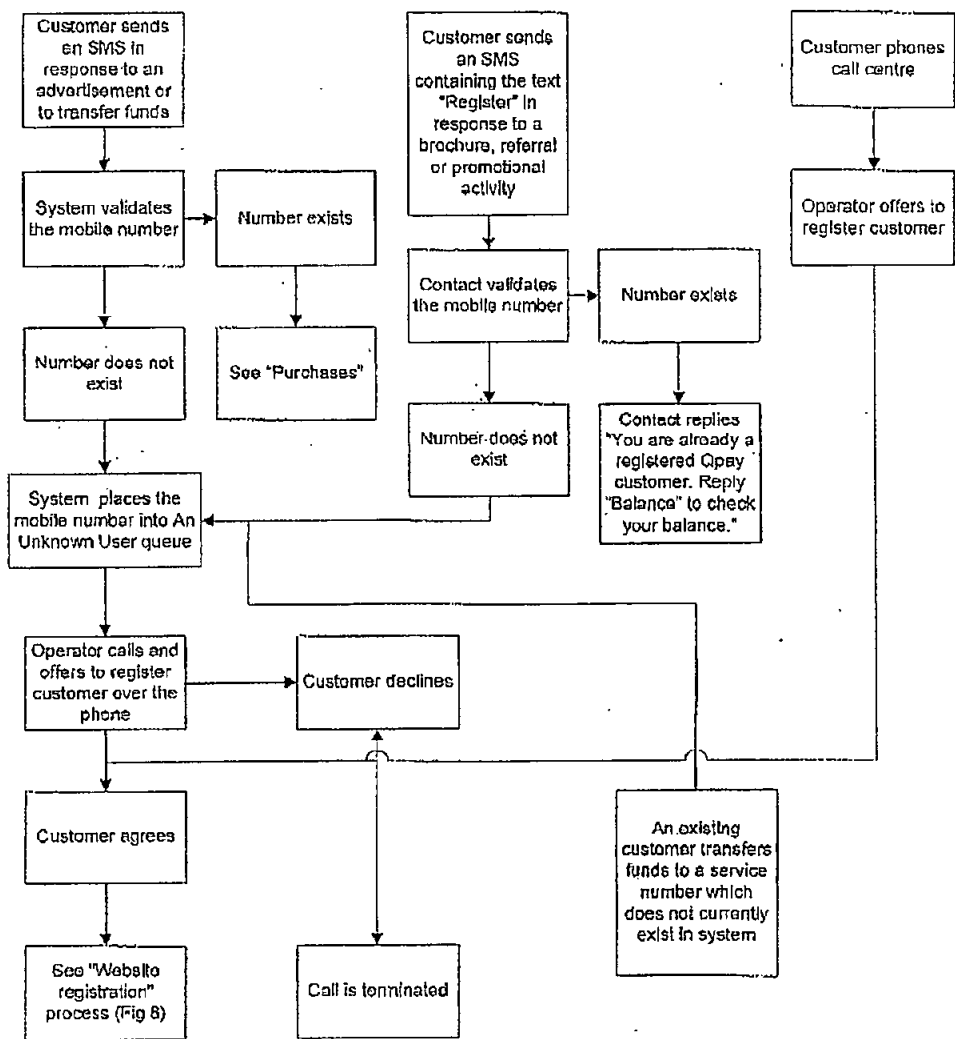


Fig. 7

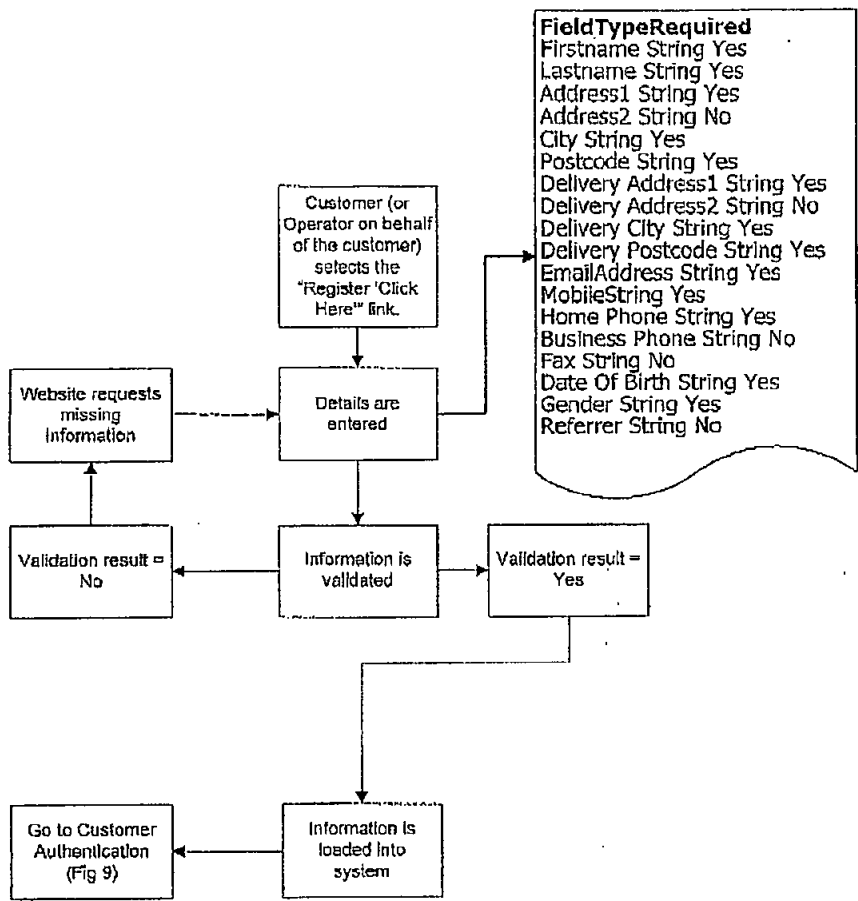


Fig. 8

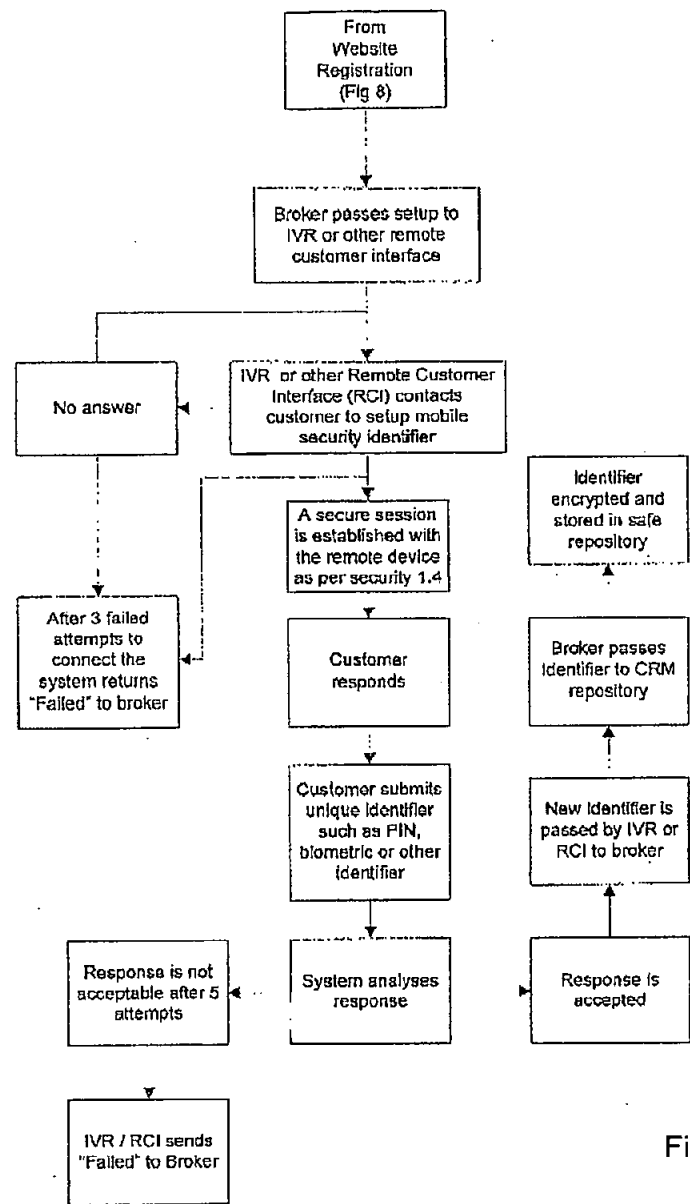


Fig. 9

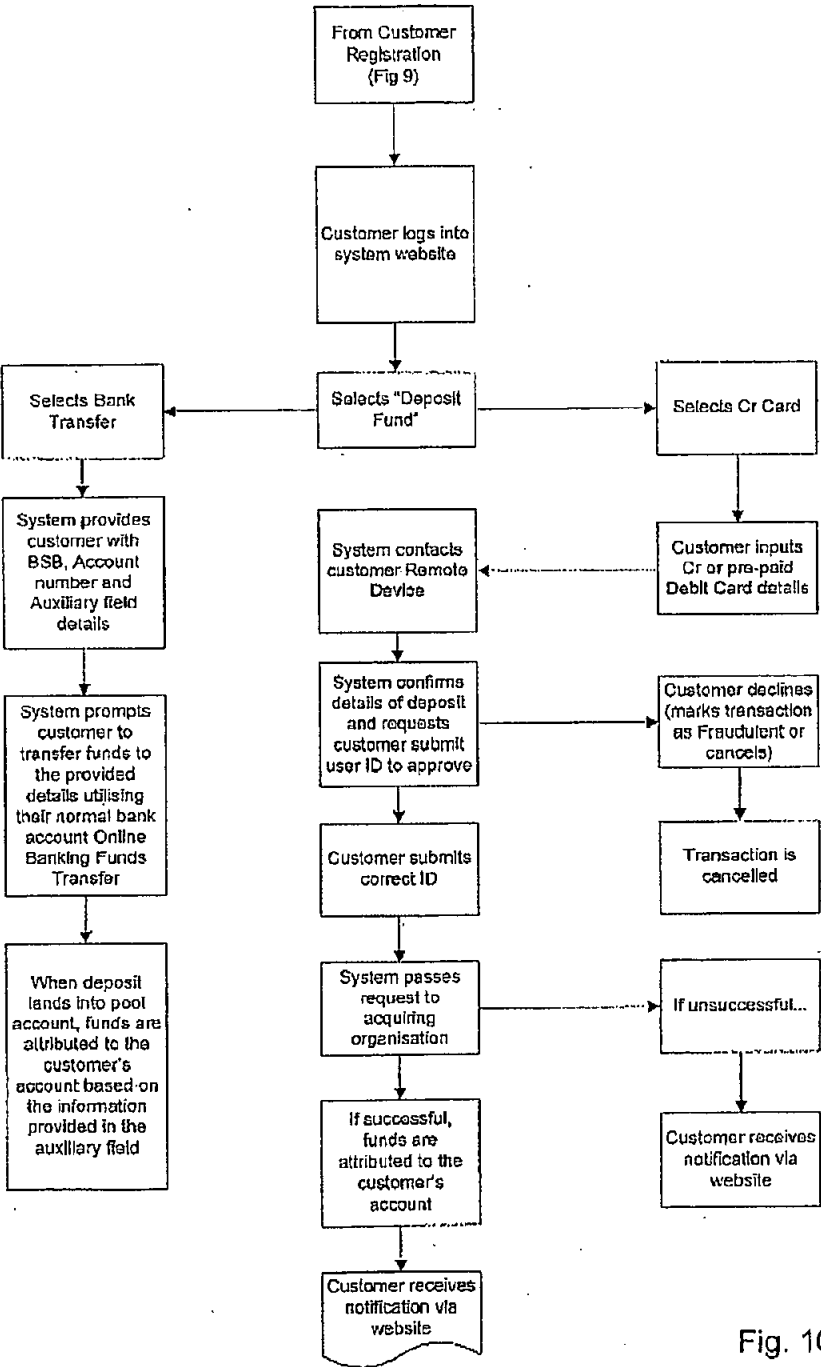


Fig. 10

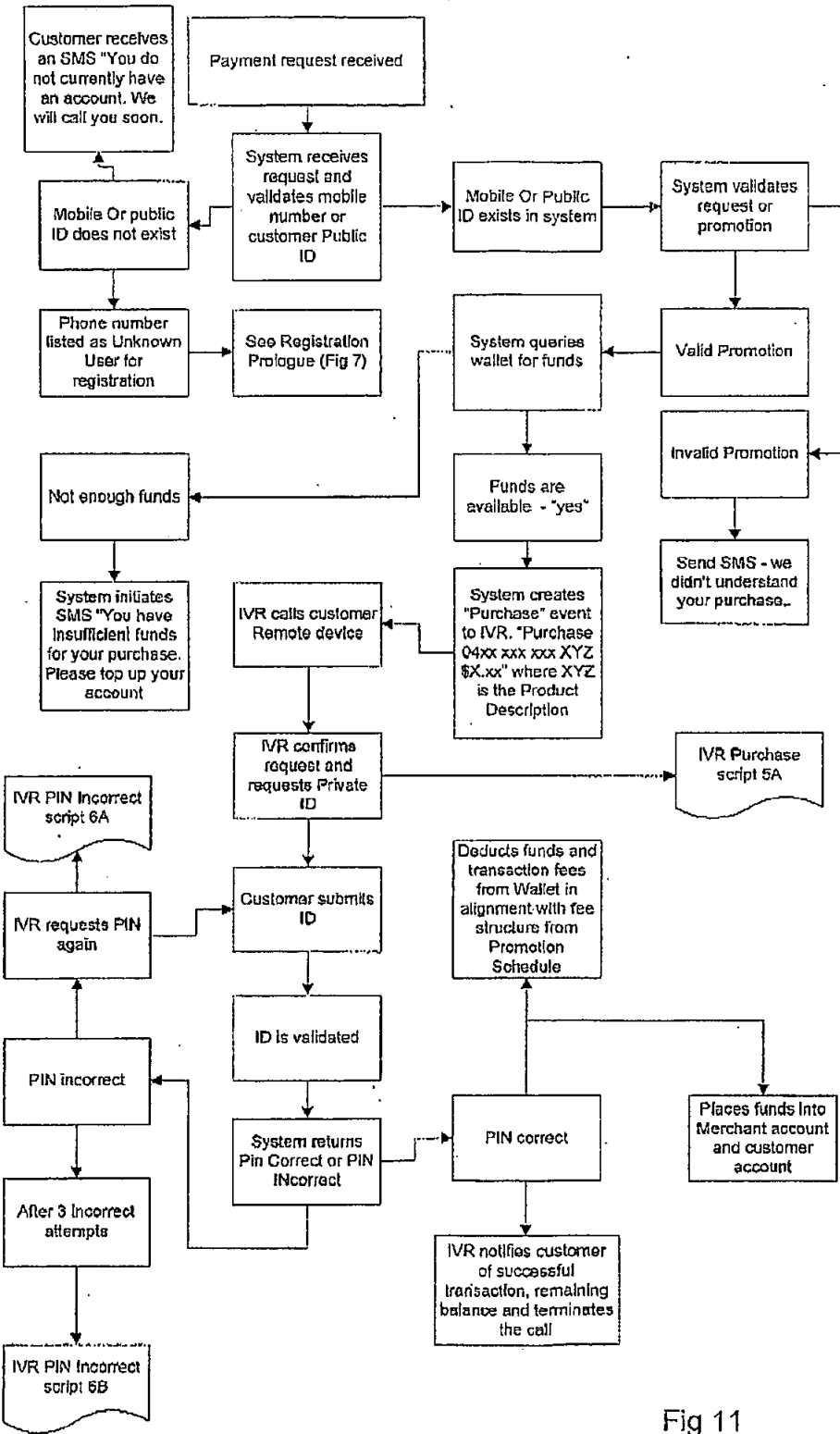


Fig 11

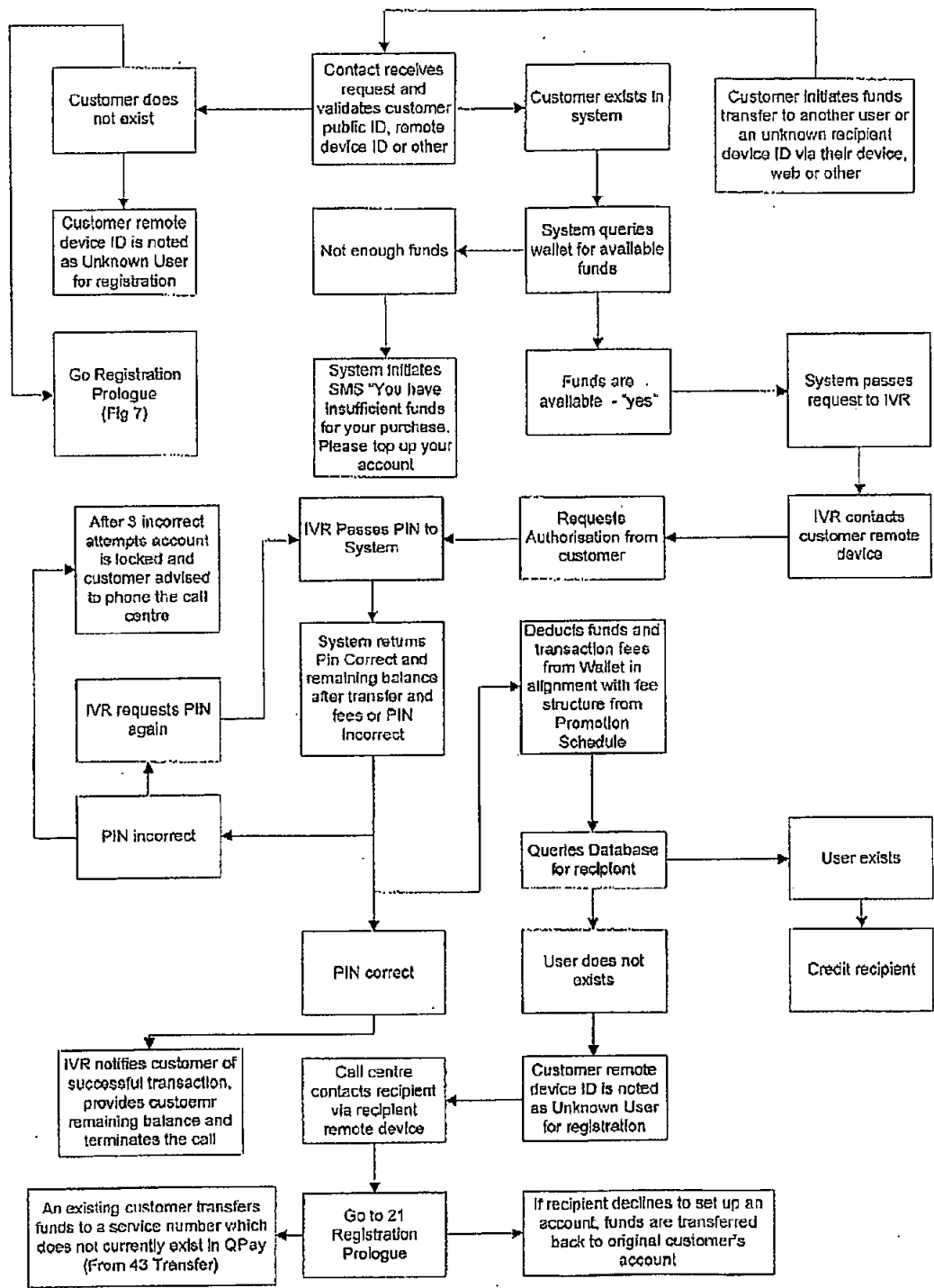


Fig 12

49

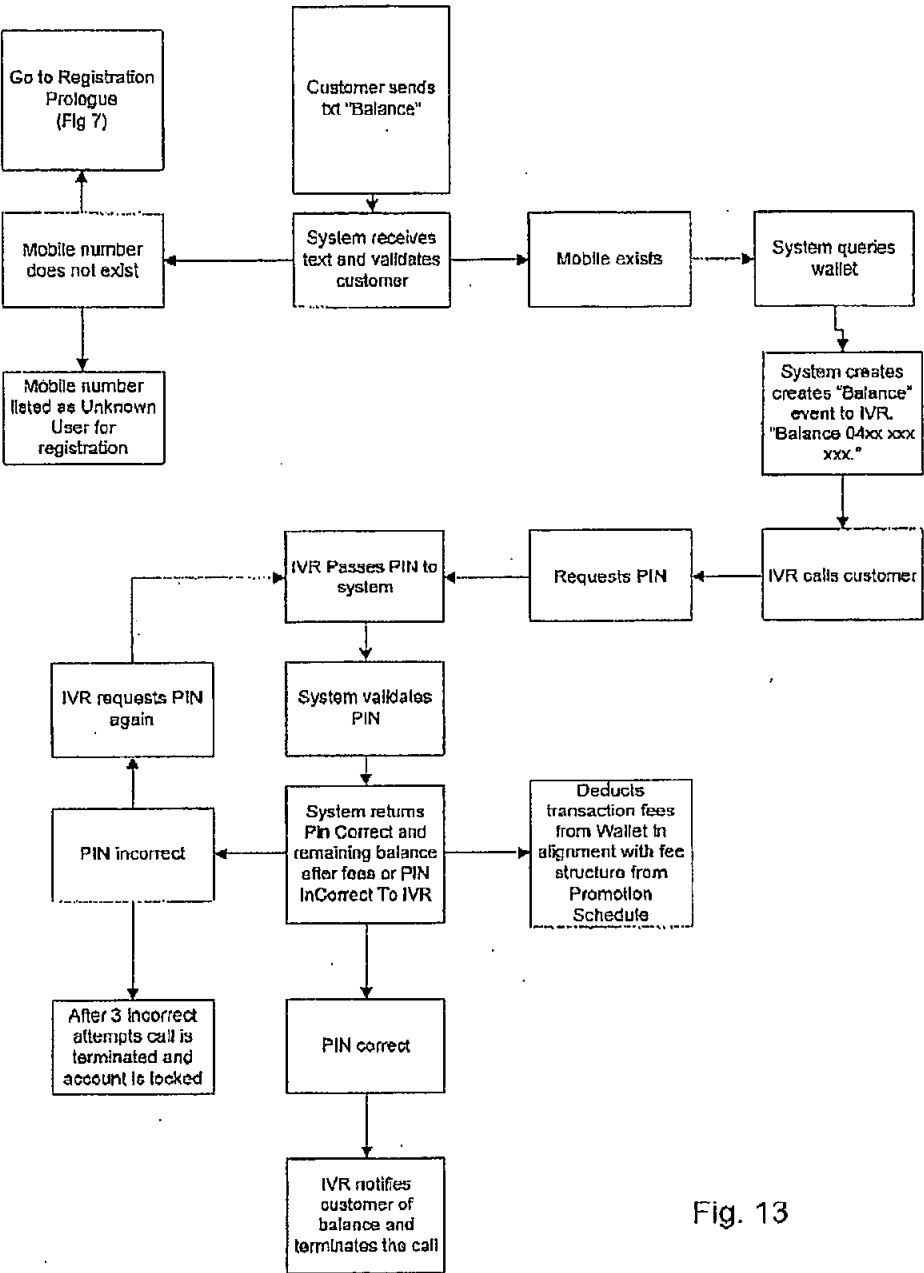


Fig. 13

INTERNATIONAL SEARCH REPORT

 International application No.
 PCT/AU2007/001076

A. CLASSIFICATION OF SUBJECT MATTER Int. Cl. G06Q 20/00 (2006.01) G06F 17/30 (2006.01) According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) EPO and DWPI using IPC and keywords including credit card, debit card, stored value card, communication device, mobile phone, confirm, authorize, password, pin, anonymize		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 399 209 A (FORTUNATUS HOLDINGS LIMITED) 8 September 2004 See whole document and particularly pages 19 and 26 to 39	1 to 25
X	GB 2 398 159 A (WILLIAMS) 11 August 2004 See whole document and particularly pages 8 to 10	1 to 25
A	US 2005/0043964 A1 (THIELSCHER et al) 24 February 2005 See whole document	1 to 25
A	US 2004/0078238 A1 (THOMAS et al) 22 April 2004 See whole document	1 to 25
☒ Further documents are listed in the continuation of Box C ☒ See patent family annex		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier application or patent but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "&" document member of the same patent family		
Date of the actual completion of the international search 12 September 2007		Date of mailing of the international search report 19 SEP 2007
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaaustralia.gov.au Facsimile No. (02) 6285 3929		Authorized officer LUKE DAVESON AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No : (02) 6283 2773

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/001076

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2001/042883 A2 (ARCANVS INC) 14 June 2001 See whole document	1 to 25
A	Patent Abstracts of Japan, JP 02-027463 A (FUJITSU LTD) 30 January 1990, (machine translation, retrieved 3 September 2007 from the internet) <URL: http://www19.ipdl.inpit.go.jp/PA1/cgi-bin/PA1INDEX> See whole document	1 to 25

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2007/001076

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report				Patent Family Member			
GB	2399209	EP	1604339	WO	2004079676		
GB	2398159						
US	2005043964	CA	2462981	CN	1602495	DE	10209780
		EP	1451736	WO	03034294		
US	2004078238						
WO	0142883	AU	45229/01	CA	2393860	EP	1240574
		US	6397224				
JP	2027463						
Due to data integration issues this family listing may not include 10 digit Australian applications filed since May 2001.							
END OF ANNEX							

SISTEMA Y MÉTODO PARA AUTORIZACIÓN DE TRANSACCIÓN

CAMPO DE LA INVENCION

5 La presente invención se relaciona con un sistema y con un método para la autorización de transacciones tal como compras con tarjetas de crédito, transferencias bancarias, y compras de acciones, particularmente en ambientes en donde se hacen pagos remotos para bienes y servicios.

10 ANTECEDENTE DE LA INVENCION

 La seguridad de las transacciones financieras y de otros tipos es de gran importancia debido al crecimiento relativamente reciente de amenazas tal como phishing (suplantación de identidad) y pharming (manipulación de direcciones de DNS) que están destinadas a adquirir fraudulentamente información delicada, tal como claves, detalles de tarjetas de crédito y números de identificación personal, al disfrazarse como una persona confiable o negocio en una comunicación electrónica. Una vez se adquieren fraudulentamente tales detalles se utilizan para hacer pagos financieros o para malversación de fondos de cuentas financieras. Frecuentemente el tenedor de la cuenta no tiene conocimiento de estas transacciones fraudulentas hasta después que ellas se han concluido y es muy tarde para intervenir. Es deseable, por lo tanto, buscar autorización de transacciones de un cliente antes que se concluyan las transacciones por la institución financiera.

25 En sistemas actuales utilizados para autorizar transacciones financieras, es difícil y frecuentemente imposible obtener una firma que garantice que la persona que inicia la transacción es el tenedor de la cuenta y está autorizado a concluir la transacción. Por

ejemplo, cuando un comerciante desliza una tarjeta de crédito de un cliente, la terminal para tarjetas de crédito se conecta al adquirente del comerciante, o procesador de tarjeta de crédito, que verifica que la cuenta del cliente sea válida y que tenga disponibles suficientes fondos para cubrir el costo de la transacción. Sin embargo, este proceso no proporciona ninguna forma de verificación de que el individuo que hace la transacción está de hecho autorizado a hacerlo.

Aunque un comerciante puede comparar una firma sobre la tarjeta de crédito con la firma del cliente, tales métodos para verificar si o no la transacción es fraudulenta están bastante lejos de ser a prueba de fallos. Adicionalmente, el tenedor de la cuenta y el proveedor de la tarjeta de crédito se basan en que el comerciante niegue las transacciones que parezcan ser fraudulentas y no autorizadas.

Este asunto es particularmente notorio con transacciones conducidas en ambientes en línea o telefónicos, en donde el comerciante es incapaz de verificar la firma del cliente y determinar por lo tanto si una transacción es fraudulenta o no.

Un método para superar tal asunto es solicitar al comprador proporcionar un código de valor de verificación de tarjeta (CVV), que no es parte del número de tarjeta en sí mismo, y también se conoce como CVV2, CVC2, y CID. El CVV es un procedimiento de autenticación establecido por compañías de tarjetas de crédito para reducir el fraude por Internet y del fraude transacciones telefónicas. Éste consiste en solicitar al tenedor de la tarjeta proporcionar el número CVV en el momento de la transacción para verificar que la tarjeta está a mano. Mientras el código CVV ayuda a comprobar que el cliente que coloca la orden posee actualmente la tarjeta de crédito/débito y que la cuenta de la tarjeta es legítima, este procedimiento de autenticación no es efectivo cuando la tarjeta en sí misma ha sido malversada o está en

escenarios en donde no ha habido acceso autorizado a los registros financieros del tenedor de la cuenta.

De manera similar, en los sistemas actuales en donde se requiere que el cliente
5 proporcione una clave o un número de identificación personal antes que se autorice acceso o no se autorice acceso a los registros del tenedor de la cuenta es probable proporcionar la información requerida para autorizar transacciones fraudulentas.

De acuerdo con lo anterior, es un objeto de la invención proporcionar un sistema
10 para autorizar transacciones que busque solucionar los problemas de los sistemas de la técnica anterior.

Se entenderá claramente que, si una publicación de la técnica anterior o sistemas mencionados aquí; esta referencia no constituye una admisión de que la
15 publicación o el sistema forma parte del conocimiento general común en la técnica en Australia o en algún otro país.

RESUMEN DE LA INVENCION

20 Ampliamente, la invención posibilita transacciones, tal como pagos con tarjeta de crédito, transferencia de fondos bancarios en línea, u otras, a ser autorizadas de manera segura por un cliente, preferiblemente antes que se concluya la transacción por la institución relevante. En una forma, tal autorización ocurre cuando el sistema de respuesta de voz interactiva (IVR) solicita al cliente, por ejemplo, que proporcione uno o
25 más identificadores únicos para validar su identidad y autenticar la transacción.

Alternativamente, el cliente puede indicar que la transacción es fraudulenta que a su vez comunica a la institución relevante de tal manera que se puedan tomar las acciones apropiadas. La información mantenida por el sistema de autorización se separa de la cuenta y los registros de cliente de la institución financiera con el fin de maximizar la seguridad en el proceso de autorización y mitigar el riesgo de autenticación fraudulenta de transacciones que puedan surgir como un resultado de acceso no autorizado a información almacenada.

En un aspecto, la invención proporciona un sistema de autorización de transacción para permitir a un cliente autorizar transacciones que se relacionen con por lo menos una cuenta de cliente asociada con una institución, el sistema incluye:

Medios de almacenamiento de datos para permitir acceso a

- (a) datos de identificación asociados con el cliente;
- (b) datos de identificación asociados con un dispositivo de comunicación remota (RCD) del cliente; y
- (c) datos de identificador de seguridad que asocian con por lo menos una cuenta de cliente con uno o ambos de (a) y (b);

Un primer medio de comunicación para permitir comunicación con el cliente por vía del RCD para autorizar una transacción sobre por lo menos una cuenta de cliente;

Una arquitectura de procesamiento de datos incluye medios de procesamiento de datos para identificar el cliente que utiliza (a), identifica el RCD utilizando (b) y determina si la transacción se autoriza por el cliente; y

5 Unos segundos medios de comunicación para recibir una solicitud de autorización en relación con la transacción y proporcionar una indicación a la institución de si se autoriza o no la transacción por el cliente, en donde la solicitud de autorización recibida y la indicación proporcionada a la institución hacen referencia a los datos de identificador de seguridad.

10

En otro aspecto, la presente invención proporciona un método para permitir a un cliente autorizar transacciones que se relacionan con por lo menos una cuenta de cliente mantenida en una institución, el método incluye las etapas de:

- 15 a) Un servidor de autorización recibe una petición de autorización de la institución en relación con una transacción sobre por lo menos una cuenta de cliente;
- 20 b) El servidor de autorización se comunica con el cliente por vía de un dispositivo de comunicación remoto (RCD) del cliente para autorizar la transacción;
- 25 c) El servidor de autorización identifica al cliente utilizando los datos de identificación asociados con el cliente para que el servidor de autorización tenga acceso;

d) El servidor de autorización identifica el RCD utilizando los datos de identificación almacenados asociados con el RCD al cual tiene acceso el servidor de autorización;

5 e) El servidor de autorización determina si se autoriza la transacción por el cliente;

f) El servidor de autorización comunica una indicación a la institución de si se autoriza o no la transacción por el cliente

10

en donde la petición de autorización recibida por el servidor de autorización y la indicación proporcionada por la institución se referencian por la institución y el servidor de autenticación para datos de identificador de seguridad para asociar por lo menos una cuenta de cliente con uno o ambos de los datos de identificación almacenados
15 asociados con el cliente y los datos de identificación almacenados asociados con el RCD.

En una forma, la invención reside en un sistema de pago remoto que permite a un cliente transar pagos por bienes y servicios de manera remota en una forma segura
20 con miembros del sistema, el sistema incluye:

i) Medios de almacenamiento de datos que contienen datos actualizables que se relacionan con cada uno de una pluralidad de clientes y cada uno de una pluralidad de miembros del sistema, en donde cada cliente tiene por lo menos
25 un perfil de registro asociado con una reserva monetaria relacionada;

- ii) Una arquitectura de procesamiento de datos que incluye medios de procesamiento de datos y un sistema de caja de compensación para liquidación de endeudamiento entre los miembros y los clientes del sistema,
- 5 iii) Medios de comunicación asociados con la arquitectura de procesamiento de datos para comunicar con el cliente por vía de un dispositivo de comunicación remoto (RCD) de cada uno de los clientes,

El sistema está dispuesto para que uno o más de dichos clientes transe pagos
10 por bienes o servicios conforme a una solicitud de pago hecha por uno o más de los miembros, la solicitud de pago activa un evento de comunicación desde los medios de comunicaciones al RCD del cliente relevante para el propósito de validar la identidad del cliente y el acceso al perfil de registro respectivo, y el sistema está dispuesto adicionalmente con el fin de validar la identidad del cliente y una que esto ha sucedido,
15 permitir al cliente transar los pagos proporcionando un balance positivo que permanece en la reserva monetaria.

En una segunda forma, la invención reside en un método de pago remoto que permite a un cliente transar pagos por bienes y servicios de forma remota de una
20 manera segura con miembros de un sistema de pago remoto, el sistema incluye:

- i) Medios de almacenamiento de datos para contener datos actualizables que se relacionan con cada uno de una pluralidad de clientes, y cada uno de una pluralidad de miembros del sistema, en donde cada cliente tiene por lo menos
25 un perfil de registro asociado con una reserva monetaria relacionada;

- ii) Arquitectura de procesamiento de datos que incluyen medios de procesamiento de datos y un sistema de caja de compensación para liquidar endeudamiento entre los miembros y clientes del sistema,
- 5 iii) Medios de comunicaciones asociados con la arquitectura de procesamiento de datos para comunicación con los clientes por vía de un dispositivo de comunicación remoto (RCD) de cada uno de los clientes,

En donde el cliente utiliza el sistema para transar pagos por bienes o servicios
10 conforme a una solicitud de pago hecha por uno o más de los miembros, la solicitud de pago activa un evento de comunicaciones de por lo menos uno de los medios de comunicaciones al RCD del cliente relevante para el propósito de validar la identidad del cliente y tener acceso al perfil de registro respectivo, y una vez se ha validado la identidad del cliente, se le permite al cliente transar pagos proporcionando un balance
15 positivo que permanece en la reserva monetaria.

El término transacción está destinado a cubrir ampliamente varias acciones que se pueden desarrollar sobre una cuenta, tal como solicitud de pago, solicitud de orden, transferencia de acciones, transferencia de fondos, solicitud de prueba de identidad,
20 solicitud de liberación de información, o una combinación de estas acciones. Tales acciones también se pueden iniciar en una variedad de formas, por ejemplo, una solicitud de pago se puede originar a partir de una transacción de tarjeta de crédito en una tienda física, una compra en un sitio de red de comercio electrónico (click-para comprar), o un sistema de pago remoto que utiliza un teléfono móvil del cliente para
25 pagar bienes y servicios tal como los sistemas "text-to-buy" (texto para comprar) o "talk-to-buy" (hablar para comprar).

El término "cliente" está destinado a ser entendido para incluir ampliamente no solo clientes de instituciones financieras, sino también cualquier persona que tenga una cuenta con una institución, por ejemplo, empleados, proveedores, o ciudadanos que se relacionan con una agencia gubernamental.

5

La invención proporciona ventajosamente al cliente una oportunidad, preferiblemente utilizando por lo menos uno de los medios de comunicación que esta "fuera de línea" y por lo tanto es menos susceptible de rupturas de seguridad, para autorizar o marcar una transacción antes que se apruebe por el banco o emisor de la
10 tarjeta de crédito, y se transfieran los fondos al comerciante.

Aunque es usualmente deseable que tenga lugar la autorización de una transacción para la finalización del proceso de transacción, es posible apreciar que la autorización de la transacción puede tener lugar en cualquier punto durante el proceso
15 de transacción. Por ejemplo, se prevé que la autorización de la transacción pueda ocurrir a un antes que se haga una petición de fondos por el comerciante. Esto es particularmente ventajoso en ambientes en línea en donde se requiere que el tiempo de procesamiento de las transacciones caiga usualmente dentro de limitaciones específicas.

20

También se prevé que la invención se puede aplicar en situaciones en donde se proporciona una autorización de preaprobación sin poner en contacto primero al cliente, permitiendo que la transacción proceda sin retraso. Sin embargo, si el cliente, una vez está en contacto con respecto a la transacción, falla en autorizar la transacción o marca
25 la transacción por no estar autorizada, la preautorización se revoca inmediatamente y si ya se han transferido los fondos, ellos también se recuperan.

Uso de un identificador de seguridad tal como un PIN que se memoriza por los medios de datos biométricos o de cliente (por ejemplo registro de voz, huella digital, exploración de retina, behaviometría, etc.) que la transacción solo se autoriza una vez se verifica la identidad del cliente, utilizando la información que no está normalmente disponible para una persona que hace fraude. Se proporciona una ventaja adicional por el hecho de que la verificación del cliente y los detalles de contacto en el sistema se mantienen en un almacenamiento de datos separados para los detalles bancarios del cliente solo con un único identificador de seguridad (conocido solo por el sistema del banco y el sistema de autorización) que enlaza los almacenamientos de datos separados. Tal una configuración proporciona seguridad incrementada cuando se solicita acceso no autorizado a uno cualquiera de los almacenamientos de datos que por sí mismo no proporcionará información adecuada para evadir el sistema de autorización y conducir transacciones fraudulentas.

El sistema de la presente invención es particularmente útil para clientes que no tienen acceso a instalaciones bancarias convencionales o aquellos que simplemente desean una forma más conveniente y segura en la que autorizan pagos para bienes y servicios, u otras transacciones de una forma segura.

Las tarifas se pueden recaudar por el administrador del sistema para transacciones efectuadas utilizando el sistema, y que pueden ser tarifas planas o porcentajes de cantidades de transacción, o una combinación de estas. El dispositivo de comunicaciones remoto (RCD) puede ser cualquier dispositivo capaz de comunicación y no se limita a dispositivos de comunicación de una vía o dos vías. Ejemplos de formas preferidas de RCD incluyen teléfonos móviles o fijos del cliente, un dispositivo de computo personal (sea móvil o fijo) o un facsímile o busca personas del

cliente. Todos estos dispositivos y otros que no se listan pero se incluyen como un RCD pueden tener generalmente un componente de software.

Cualquier RCD que un cliente desee utilizar con el sistema se debe registrar con el sistema y de acuerdo con lo anterior, la información que identifica el RCD (que normalmente es único para ese RCD) se registra para uso en el proceso de identificación.

El cliente puede designar que RCD o grupo de RCD desean ellos utilizar para contactar el sistema y si se designa un grupo, por ejemplo, para autenticación multifactor (discutido adelante), el cliente puede designar adicionalmente que RCD es el que se ejecuta en que forma dentro del proceso de identificación multifactor.

La autorización para una transacción particular será dependiente de la validación de la identidad del cliente que se requerirá típicamente antes de la autorización para que se de la transacción. El sistema establece la verificación de la identidad del cliente como una condición de preautorización, y la transacción se bloqueará preferiblemente antes de la autorización si no se satisface la condición. En otras palabras, la transacción se declinará si la identidad del cliente no se puede establecer por el sistema. Se puede enviar una alerta al administrador del sistema, que notifica al administrador del sistema de la falla en verificar la identidad del cliente, que permite las etapas de rechazo o bloqueo de la transacción solicitada.

Usualmente, se da generalmente autorización para transacciones por instituciones financieras dependientes de la satisfacción del parámetro de identificación y/o otros parámetros mientras que la cantidad de transacción no excede el límite de crédito y/o la membresía esta aún valida y similares. El sistema de la invención puede

operar como una parte adicional de este proceso de autorización. El sistema se puede asociar con la alimentación de datos utilizada durante el proceso de autorización y la satisfacción o contravención del criterio de identificación comunicado al administrador del sistema puede ser un parámetro adicional que se puede requerir antes de que se de
5 la autorización por la institución financiera.

En el contexto de una transacción de tarjeta de crédito común, por ejemplo, el cliente, quien es típicamente el propietario de la tarjeta, utiliza la tarjeta para hacer una compra a un comerciante, que es el negocio que acepta los pagos de tarjeta de crédito
10 por los productos o servicios vendidos al cliente. El comerciante recolecta generalmente la información de la tarjeta, al deslizar la tarjeta a través de un lector o máquina similar si es una tienda física, o de otra forma por vía de Internet o por vía telefónica.

Cuando el comerciante desea verificar, por ejemplo, que la tarjeta es válida y el
15 cliente de la tarjeta de crédito tiene suficiente crédito para cubrir la compra, se conduce una verificación electrónica utilizando la terminal de pago de la tarjeta de crédito, el Sistema de Punto de Venta (POS) o similares con un enlace de comunicaciones al banco adquiriente del comerciante. Los datos de la tarjeta se obtienen de una banda magnética o chip sobre la tarjeta, un chip sobre un dispositivo de cliente, o está provisto
20 por el cliente en una forma en línea o verbalmente por teléfono.

El adquiriente, es decir la institución financiera u otra organización que proporciona servicios de procesamiento de tarjetas para el comerciante, contacta al emisor de la tarjeta por vía de la asociación de tarjeta, es decir una red tal como VISA o
25 MasterCard (y otros) que actúa como un portal entre el adquiriente y el emisor para autorizar y fondear las transacciones.

El emisor, preferiblemente antes de autorizar y fondear la transacción, reenvía la solicitud al sistema de la presente invención para autorización del cliente.

Se apreciará, que tal petición de autorización de cliente no se limita a los sistemas de pagos que involucran tarjetas de crédito, pero se puede aplicar igualmente a sistemas de transacción financiera que involucran tarjetas débito, transferencias de fondos entre cuentas, compras de acciones, etc., o por ejemplo, cuando se accesan a sistemas de seguridad a través de una red y se emite una petición con el propósito de autorizar el acceso al sistema remoto.

También se prevé y describe en detalle adelante un sistema de pago remoto completo en el que se recibe petición de autorización del cliente y se procesa directamente por el sistema.

De manera importante, independiente de la forma en la que se haga el contacto para el pago utilizando el sistema, las porciones esenciales del proceso de autenticación y validación tendrán lugar preferiblemente empezando con el sistema de contacto al RCD designado del cliente y utilizando preferiblemente un sistema de respuesta de voz interactivo (IVR) o sistema similar para verificar la identidad del cliente. El proceso de autenticación puede incluir uno o más factores y métodos de contacto con el cliente y la autenticación que incluye, pero no se limita a, sistemas IVR, información biométrica que se relaciona con el cliente tal como reconocimiento de voz en particular, entrada de códigos de uno o más fuentes junto con uno o más canales de comunicación, códigos generados, ID de frecuencia de radio (RFID), códigos de una sola vez o similares.

Se puede utilizar autenticación de dos factores en un intento por superar nuevas formas de fraudes, tiene que utilizar dos rutas de comunicaciones diferentes. Por ejemplo, el sistema puede comunicar un reto al teléfono celular del cliente por vía SMS y espera una respuesta específica. Si se asume que todos los clientes del banco tienen
5 teléfonos celulares entonces esto resulta en un proceso de autenticación de dos factores sin hardware extra. La autenticación multifactor involucrará típicamente el uso de más de un canal o sesión de comunicaciones en donde se puede emitir un reto sobre un primer canal y, la respuesta del cliente o segunda pieza de autenticación se comunica sobre un canal de comunicaciones diferente o sesiones de comunicación
10 diferente que el primero, que requiere que el cliente tenga acceso a ambos con el fin de completar, haciendo la indiscreción mucho más difícil. Los canales de comunicaciones se dirigirán típicamente a un RCD de particular que en sí mismo tendrá normalmente información de identificación única que también se requerirá para coincidir o correlacionar la información de verificación del cliente almacenada en el sistema antes
15 que se otorgue la autenticación.

El sistema utiliza la petición de autenticación como la base para poner en contacto al cliente por vía del dispositivo de comunicación del cliente en por lo menos un RCD utilizando una pregunta de entrada de datos. La pregunta de entrada de datos
20 puede ser un mensaje que requiere la entrada de información de identificación privada particular (ID privada) tal como un código y otros datos de verificación, una entrada original que se crea por el cliente o se genera cuando la cuenta del cliente se enlaza inicialmente al sistema y que se puede cambiar cuando se requiera.

25 La información que se relaciona con una o más ID privadas y uno o más RCD del cliente se almacenan por el sistema, pero se mantienen separados de la información de cuenta del cliente que se mantiene por los sistemas de institución relevante. La

información que se relaciona con un cliente particular en el sistema y los sistemas de la institución financiera utilizan un identificador de seguridad único (ID de seguridad) que no se relacionan necesariamente con una característica de identificación del cliente o RCD del cliente, y no se requiere que se proporcione al cliente.

5

El sistema compara la información ID privada recibida del cliente, o aspectos de la información suministrados, conforme a la pregunta de entrada de datos, para los datos de identificación privados mantenidos por el sistema para propósito de verificación. Ventajosamente, los datos de identificación privados respectivos del cliente y aquellos almacenados en el sistema se aseguran con mecanismos de encriptación tal como "hashing".

10

La forma de contacto más preferida con el cliente para propósitos de autenticación es el sistema que utiliza un componente de respuesta de voz interactivo (IVR), que es un sistema computarizado que permite a una persona, típicamente una persona que llama por teléfono, seleccionar una opción de un menú de voz y de otra forma de una interfaz con un sistema de computador. Generalmente el sistema reproduce preguntas de voz pregrabadas para que la persona presione un número sobre un teclado de teléfono para seleccionar una opción, o da respuestas simples tal como "sí" "no", o números en respuestas a la pregunta de voz.

15

20

Los últimos sistemas utilizan reconocimiento de voz de lenguaje natural para interpretar las preguntas que la persona desea responder. La tendencia más nueva es la Charla Guiada IVR que integra agentes humanos vivos en el diseño y flujo de trabajo de la aplicación para ayudar al reconocimiento de la charla con contexto humano. Se puede utilizar el IVR desarrollado como un sistema de telefonía pero están ahora

25

disponibles sistemas similares que funcionan sobre sistemas de no telefonía y ningún sistema funcionalmente equivalentes o combinaciones de sistemas

Típicamente, se incluye un componente IVR en por lo menos unos medios de comunicación y sobre la arquitectura de procesamiento de datos que reciben una pregunta de autenticación, el componente IVR contactará típicamente al cliente utilizando su dispositivo de comunicación remoto preferido (RCD). Probablemente el RCD será un teléfono móvil o similar y el sistema IVR puede guiar entonces al cliente a través de la entrada de su información de identificación para ser utilizado en el proceso de autenticación. De manera importante, los medios de comunicación del sistema también tendrán típicamente la capacidad de determinar las características de identificación de los medios de comunicación remotos particulares utilizados, tal como números de tarjeta SIM o direcciones IP, o certificados digitales y similares con el fin de identificar al cliente de acuerdo con un proceso de autenticación multifactor.

15

Si los datos de verificación ingresados, coinciden o se correlacionan con los datos de verificación en archivo, entonces se considera que el cliente es valido para autorizar la transacción. Si los datos de verificación ingresados, no coinciden o se correlacionan con los datos de verificación en archivo, entonces se considera que el cliente no es valido y se rechaza del sistema.

20

La entrada inválida de los datos de verificación también puede marcar un seguimiento del administrador del sistema. Preferiblemente, una vez se ingresan los datos de verificación inválidos un número de veces predeterminado, que puede ser de por lo menos una vez pero preferiblemente no más de tres veces, ese cliente puede quedar fuera del sistema durante un periodo de tiempo. La salida se puede activar en la cuenta del cliente o se puede limitar a la salida de acceso del sistema de medios de

25

comunicación remotos particulares utilizados por el cliente como se determina utilizando las características de identificación de los medios de comunicación remotos particulares utilizados.

- 5 Una vez la autenticación se otorga o se rechaza, se proporciona una indicación apropiada a las instituciones financieras relevantes y un mensaje adecuado informa al cliente del resultado del proceso de autenticación que se genera preferiblemente por la arquitectura de procesamiento de datos y se reenvía al RCD preferido del cliente.

10 **BREVE DESCRIPCIÓN DE LA INVENCION**

Se describirán ahora modalidades preferidas de la presente invención con referencia a los dibujos acompañantes, en los cuales:

- 15 La Fig. 1 es un diagrama de contexto que proporciona una descripción de una modalidad preferida de la invención;

La Fig. 2 es un diagrama de flujo que destaca el proceso de configuración de una modalidad preferida de la invención;

20

La Fig. 3 es un diagrama de flujo que destaca el proceso de autorización de una modalidad preferida de la invención;

- La Fig. 4 es un diagrama de flujo que destaca el proceso de cambio de
25 dispositivo de una modalidad preferida de la invención;

La Fig. 5 es un diagrama de flujo que destaca el proceso de cambio de identificador de cliente de una modalidad preferida de la invención;

La Fig. 6 es un diagrama de contexto que proporciona una descripción de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención;

La Fig. 7 es un diagrama de flujo que destaca un proceso de registro de cliente de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención.

La Fig. 8 es un diagrama de flujo que destaca un proceso de registro en sitio de red de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención;

15

La Fig.9 es un diagrama de flujo que destaca un proceso de autenticación de cliente de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención;

La Fig. 10 es un diagrama de flujo que destaca un primer proceso de depósito de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención;

La Fig. 11 es un diagrama de flujo que destaca un proceso de compra de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención;

La Fig. 12 es un diagrama de flujo que destaca un proceso de transferencia de fondos de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención; y

5 La Fig. 13 es un diagrama de flujo que destaca un proceso de pregunta de balance de un sistema de pago remoto que incorpora una modalidad preferida de la presente invención.

DESCRIPCIÓN DETALLADA DE LA MODALIDAD PREFERIDA

10

La presente invención no es específica para cualquier implementación de software o hardware particular, y está en un nivel conceptual sobre las especificaciones de implementación. Se debe entender que varias otras modalidades y variaciones de la invención se pueden producir sin apartarse del espíritu o alcance de la invención. La
15 siguiente se proporciona para ayudar a entender la implementación práctica de las modalidades particulares de la invención.

El sistema de autorización 20, como se muestra en la Fig. 1, incluye medios de procesamiento de datos, es decir servidor 22, con medios de comunicación 26 que
20 comunican con un sistema de institución 10 de una institución 50 y un dispositivo de cliente 30 de un cliente 40. El cliente 40 es generalmente un cliente de la institución 50, pero puede ser un empleado, proveedor, ciudadano que se relaciona con una agencia gubernamental o similar. En varias circunstancias, por lo tanto, el cliente 40 se puede identificar por el sistema de la institución 10 utilizando cualquier forma de datos de
25 identificación públicos (ID Públicas), tal como número de cuenta, número de tarjeta débito/crédito u otra tarjeta, número de empleado, nombre de inicio de sesión, clave, u

otro identificador adecuado. En algunos casos, se puede utilizar una combinación de estos identificadores como una ID Pública.

La información de identificación que se relaciona con, por ejemplo la institución 5 50, el dispositivo de cliente 30 y el cliente 40, se almacenan de forma segura en la base de datos 24 del sistema de autorización 20. La base de datos 24 puede tomar una cualquiera de varias formas, por ejemplo, una base de datos central única, una base de datos distribuida o un número de base de datos seguros.

10 Se apreciará que mientras el sistema de autorización 20 se describe en el contexto de una institución financiera, tal como un emisor de tarjetas de crédito, la institución 50 puede ser un organismo que requiera autorización segura de una transacción. Ejemplos de tales instituciones incluyen un empleador, banco, agencia del gobierno, agente de bolsa o cualquier otra entidad que este buscando identificación 15 segura o autorización.

También se apreciará que mientras el sistema de autorización 20 se describe en el contexto de una transacción financiera, la transacción puede tomar otras formas adecuadas, tal como por ejemplo, una petición para identificación del cliente 40. 20 Ejemplos de transacciones que requieren autorización por el sistema de autorización 20 incluyen una transacción financiera en línea o sobre el mostrador, una petición para aprobar una compra o venta de acciones o una petición para identificación que se puede requerir por el cliente 40 para ingresar a un edificio, abrir una cuenta, o tratar con una institución o agencia gubernamental.

25 En una forma, el sistema de autorización 20 y el sistema de institución 10 se pueden alojar en el mismo ambiente seguro para minimizar las oportunidades de

comunicación entre ellos que se interceptan por una parte no autorizada o si el sistema de autorización 20 se incorpora por la institución 50 en su propia capa de procesamiento segura.

5 Sin embargo, en donde el sistema de autorización 20 y el sistema de institución 10 se alojan en ambientes físicos separados, las comunicaciones entre ellos se deben facilitar preferiblemente por vía de un enlace seguro tal como una conexión directa, utilizando preferiblemente tecnologías "fuera de red" (es decir no basados en Internet o red) tal como una estructura o un punto seguro para conexión de punto. Cuando el 10 sistema de autorización 20 y el sistema de institución 10 se comunican por vía del uso de tecnologías "en red", se deben utilizar preferiblemente métodos de autenticación y encriptación fuertes, tal como formación de túnel VPN con autenticación de reto o tecnología similar tal como certificados Clientes/Servidor. En tales casos, se prefiere que los datos se comuniquen a través de la conexión que se encripta con una 15 inscripción mínima de 128 bit. Se puede proporcionar seguridad adicional al autenticar los paquetes de datos utilizando un algoritmo HMAC (código de autenticación de mensaje hash codificado) en el que el sistema de institución 10 está provisto con una clave secreta y toda la información enviada por el sistema de institución 10, se le realiza algoritmo hash contra la clave para autenticar los datos. Adicionalmente, las capas de 20 seguridad adicionales para datos transmitidos también se puede agregar si se requiere, tal como por ejemplo hardware de encriptación.

Se prefiere que los cambios al sistema de autorización 20 se deben registrar automáticamente y mantener dentro de un rasgo de auditoría segura que no se puede 25 cambiar aún en un nivel de acceso de administración o privilegiado y debe estar disponible en un formato de informe.

Si el sistema de autorización 20 y el sistema de institución 10 se colocan de manera segura o se conectan remotamente de forma segura, un único identificador de seguridad, denominado adelante como ID de Seguridad se utiliza para correlacionar la información que se relaciona con el cliente 40 en el sistema de autorización 20 y el sistema de institución 10, una vez se establece el procedimiento, como se muestra en la Fig. 2, que se ha completado para un nuevo usuario. La ID de seguridad niega la necesidad de transmitir constantemente información de identificación a cerca del cliente 40 o el dispositivo de cliente 30 (discutido adelante) que puede ser más fácilmente reconocido por terceras partes.

10

En esta forma la información de cuenta del cliente 40, almacenada en el sistema de institución 10, se mantiene sustancialmente independiente del sistema de autorización 20.

15

En otras palabras, el uso del ID de Seguridad asegura que si el sistema de autorización 20 y el sistema de institución 10 se atacan exitosamente y los registros del cliente 40 se accedan por una parte no autorizada, hay oportunidad mínima para que el atacante obtenga el conjunto de información completo, y más específicamente, identificadores requeridos para completar una transacción, que se discute en mayor detalle adelante.

20

Con el fin de maximizar la seguridad de las comunicaciones y la información almacenada dentro de la base de datos 24, se prefiere que la ID de Seguridad no esté visible al cliente 40, o los centros de llamada para la institución 50 o el sistema de autorización 20.

25

Con el fin de facilitar la correlación de los datos transmitidos con los datos almacenados por el sistema de institución 10, la ID de Seguridad se puede correlacionar de una forma segura con un identificador único existente utilizado por el sistema de institución 10, tal como por ejemplo, un número de cuenta del cliente 40. De manera similar, la ID de Seguridad se puede correlacionar en una forma segura con un
5 único identificador dentro de un sistema de autorización 20, que es visible a los centros de llamada, etc.

Durante el proceso de configuración de cliente en el sistema 20, la institución 50
10 pasa el ID de dispositivo al sistema 20. El sistema 20 pone en contacto el cliente 40 (por vía del dispositivo 30) "fuera de red". En este punto el cliente 40 es capaz de seguir las etapas requeridas para establecer por lo menos una ID de cliente. El sistema 20 pasa luego de nuevo a la institución 30 el dispositivo ID, y un nuevo identificador de seguridad único (ID de Seguridad). Después, el único identificador que se relaciona con
15 el cliente 40 y/o el dispositivo 30, que pasa entre la institución 50 y el sistema 20, es la ID de Seguridad.

Por lo tanto, para un usuario que hace fraude que busca obtener acceso no autorizado a un conjunto de datos completos, necesitaría una ID Pública 40 de cliente,
20 la ID de dispositivo y la ID de cliente. Para obtener toda esta información, ellos necesitarían atacar y obtener acceso no autorizado al sistema de institución 10, seguir una transacción al sistema de autorización 20 y atracar el enlace entre el sistema 20 y el dispositivo de cliente 30. Por lo tanto, en un conjunto de ejemplo en el contexto bancario, el usuario no autorizado necesitaría atacar y obtener acceso no autorizado al
25 banco, el sistema de autorización 20 y la red telefónica móvil sobre la que se conecta el dispositivo 30.

En una situación de transacción financiera típica, como se muestra en la Fig. 3, el comerciante u organización similar solicitarán a la institución 50 autorización de la transacción. En algunos casos, en donde tal autorización no se requiere por el comerciante o cuando las transacciones son internas a la institución 50, la institución 50 puede por sí misma pedir autorización de la transacción. Es en este punto que el sistema de institución 10 envía una petición de autorización 15 al sistema de autorización 20, que a su vez entra en contacto con el cliente 40 para autorización de la transacción.

10 Cuando el sistema de autorización 20 se conecta a un número de instituciones y/o sistemas de institución, la petición de autorización 15 puede incluir un único identificador para identificar la institución 50, denominada aquí como ID de institución, que se comunica con el sistema de autorización 20 con la petición de autorización 15. En situaciones, por ejemplo, en donde la institución 50 aloja el sistema de utilización 20, 15 la ID de institución puede no ser necesaria. También, se apreciará que la ID de institución puede estar en diferentes formas tal como el protocolo de Internet (IP) o dirección de control de acceso medio (MAC) de un servidor, o una combinación de números de identificación y/o letras.

20 El cliente 40 se conecta por el sistema de autorización 20 sobre el dispositivo de cliente 30. El dispositivo de cliente 30 puede ser un dispositivo portátil tal como un teléfono móvil o asistente de datos personales (PDA), o un computador portátil tal como un laptop. Se pretende que el cliente 40 se ponga en contacto con un dispositivo portátil que lleva el cliente 40 ya que esto asegurará que las transacciones se puedan autorizar 25 como se requieran y sin retraso innecesario.

Se prefiere que la comunicación con el dispositivo de cliente 30 se conduzca sobre una red de comunicación fuera de red (es decir tecnología no basada en Internet o red), particularmente en situaciones en donde la transacción en sí misma se haya conducido sobre el Internet o la red. De esta forma, aún si la sesión de transacción está comprometida, el proceso de autorización permanece seguro ya que se lleva a cabo sobre una red de comunicación diferente y por lo tanto no es probable que también esté comprometida. También, cuando una red de comunicación, que es la misma que aquella sobre la cual se conduce la transacción se utiliza, el proceso de autorización se puede conducir sobre una sesión separada a la sesión de transacción o se puede afectar en sí misma sobre más de una sesión de comunicación.

Con el fin de establecer una sesión de comunicación segura dentro del sistema de autorización 20 y un dispositivo de cliente 30, se adoptan medidas de seguridad adecuadas. La naturaleza exacta de aquellas medidas de seguridad se determinarán por supuesto por el tipo de dispositivo, el método de conexión utilizado y el tipo de red.

Por ejemplo, en el caso de teléfonos móvil GSM, un Ki 128 bit dentro de la SIM del móvil se utiliza para identificar únicamente el dispositivo para la red. Se proporciona un reto aleatorio de 128 bit (RAND) por la red con el dispositivo que luego proporciona una respuesta de 32 bit (SRES). Una clave de cifrado de 64 bit (Kc) crea una base para la encriptación durante la sesión. Los algoritmos subyacentes incluyen A3 (autenticación), A5 (encriptación) y A8 (generación de claves), y otras capas de seguridad según se requieran.

En el caso de un dispositivo CDMA, el número de serie electrónico y un programa de clave A programado en el teléfono se utilizan para identificar únicamente el dispositivo a la red. Se genera un número binario aleatorio (RANDSSD) por la red con

el dispositivo que responde con una subclave de 128 bit llamada Dato Secreto Compartido (SSD). Se utiliza la parte del SSD para autenticación, y parte para encriptación, y se pueden incluir algoritmos subyacentes estándar CAVE, CMEA, E-CMEA, o ORYX en el caso de los datos. En adición a lo anterior, se puede utilizar

5 CDMA2000 y WCDMA para aplicar capas adicionales de seguridad tal como SHA-1, AES, los algoritmos Kasumi y Rijndael y el protocolo AKA.

En el caso en que tecnologías Wi-Fi (tecnología base 802.11), Bluetooth® y otras tecnologías de Comunicación de Campo Cercano, así como también tecnología de

10 comunicación de rango alto, se utilizan para comunicar con el dispositivo de cliente 30, es preferible implementar prácticas de seguridad fuertes disponibles con tales tecnologías.

Con el fin de identificar el dispositivo de cliente 30 con el sistema de autorización

15 20, un identificador de dispositivo único, denominado aquí en adelante como ID de dispositivo, del dispositivo de cliente 30 se puede comparar con la ID de dispositivo proporcionada por el dispositivo de cliente 30. Ejemplos de tales identificadores incluyen un número de teléfono, una identidad de equipo móvil internacional (IMEI) que es un número único para cada GSM y teléfono móvil UMTS, dirección IP o MAC, o cualquier

20 otra forma o combinación que identifique únicamente el dispositivo de cliente 30 con el sistema de autorización 20.

Se apreciará que en algunos casos, por ejemplo, en donde la ID de dispositivo incluye un número de teléfono, la información allí se utilizará también para iniciar una

25 comunicación con el dispositivo 30. Sin embargo, cuando la ID de dispositivo consiste solo de identificadores de dispositivo tal como direcciones MAC, las cuales en sí mismas no son capaces de ser utilizadas para iniciar una comunicación con el

dispositivo 30, la información de contacto adicional para comunicación con el dispositivo 30 también se puede almacenar por el sistema 20.

El sistema de autorización 20 proporciona un procedimiento, como se muestra en la Fig. 4, para cambiar la ID de dispositivo almacenada en la base de datos 24, por ejemplo, si el cliente 40 obtiene un nuevo dispositivo de cliente 30.

Con el fin de autorizar las transacciones, se le pregunta al cliente 40 mediante el sistema de autorización 20 que proporcione por lo menos un único identificador de cliente, aquí en adelante denominado como ID de cliente, que se utiliza para asegurar que es el cliente actual que aprueba la transacción, y no otra persona que simplemente puede tener acceso al dispositivo de cliente 30. De manera ideal, la ID de dispositivo y la ID de cliente se aseguran de manera separada y pueden sufrir procesos de encriptación tal como "hashing" durante almacenamiento y/o comunicación.

15

La ID de cliente puede ser un número de identificación personal (PIN) o frase de clave/paso que es conocida por el cliente 40, un identificador biométrico tal como registro de voz, una palabra secreta, una huella digital o cualquier otra forma de identificador que pudiera usualmente solo ser conocida por, o accesible por, el cliente 40.

20

En forma preferida, un sistema de respuesta de voz interactivo (IVR), es decir sistema IVR 28 se puede utilizar para preguntar al cliente 30 por el ID de cliente y posteriormente recibir la ID de cliente. Un IVR es un sistema computarizado que permite al cliente 40 seleccionar opciones de un menú de voz e interactuar de otra forma con el sistema de autorización 20. De manera general el sistema IVR 28 hace una pregunta de voz prerregistrada y el cliente 40 presiona un número sobre un teclado de teléfono para

25

seleccionar una opción y/o dar una respuesta, tal como la ID de cliente, que se reconoce por el sistema IVR 28.

Por ejemplo, una ID de cliente que incluye un PIN de 4 dígitos (o 6), no se
5 conoce o almacena por el sistema de autorización 20 en una forma utilizable
digitalizada. Cuando el sistema IVR 28 recibe el DTMF por vía del PIN dentro de la
sesión asociada con la llamada, este se encripta en la sesión utilizando MD5, y esta
solo esa cadena MD5 encriptada hash, que se asocia con el PIN, que se comunica de
nuevo con el sistema de autorización 20 para validación o almacenamiento. Este
10 procedimiento asegura que en un evento improbable que el sistema de autorización 20
se ha atacado, y el atacante sea capaz de romper la encriptación que relaciona la ID de
cliente con la ID de dispositivo, ellos no sean capaces de simular una llamada de
autorización en un intento por obtener el PIN en forma utilizable para un sistema IVR a
menos que se reverse la encriptación MD5. Adicionalmente, las capas de seguridad
15 adicionales para los datos también se pueden agregar si se requieren, tal como por
ejemplo hardware de encriptación.

En una modalidad alterna, que utiliza biométricas de voz, la ID de cliente se
forma por el registro de voz del cliente 40. Este registro de voz se puede calcular al
20 pedir al cliente que repita una palabra generada aleatoriamente o frase tal como
“amarillo” que permite que el registro de voz del cliente 40 sea capturado.
Preferiblemente, una petición de autorización futura solicitará al cliente 40 que diga una
palabra diferente o frase tal como “martes” para seguridad mejorada.

25 De esta forma, el sistema de autorización 20 determina el registro de voz
biométrica de la respuesta y la compara con los datos almacenados. Como otra capa de
seguridad, el sistema 20 también puede desarrollar una conversión de voz a texto de la

palabra o frase y hacer una comparación adicional con los datos almacenados para confirmar que la palabra dicha es de hecho una registrada. Por lo tanto, para romperse, un usuario que busca acceso no autorizado requeriría no solo una alta calidad de registro de la voz del cliente sino también necesitaría utilizar ese registro para decir la
5 palabra aleatoria solicitada.

En otra modalidad alterna, el sistema 20 puede hacer al cliente 40 una pregunta para que el o ella conozca probablemente la respuesta. Por ejemplo, el sistema 20 puede preguntar “cuándo fue su última transacción?”, o “cuál es su segundo nombre?”.
10 La respuesta del cliente 40 se compara no solo contra los datos impresos de voz almacenada sino que también se determina la exactitud de la respuesta.

Una vez se proporciona la ID de cliente por el cliente 40, se puede considerar la transacción por el sistema de autorización 20 como autorizada. De acuerdo con lo
15 anterior, el sistema de autorización 20 comunica la autorización de la transacción al sistema de institución 10, que a su vez permitirá a la institución 50 tomar las acciones apropiadas para concluir la transacción.

El sistema de autorización 20 proporciona un procedimiento, como se muestra en
20 la Fig. 5, para cambiar la ID de cliente almacenada en la base de datos 24, por ejemplo, si el cliente 40 necesita cambiar su clave, PIN, etc.

En ciertas situaciones, el cliente 40 puede necesitar proporcionar una respuesta al sistema de autorización 20, en cambio de, o en adición a, la ID de cliente. Esta
25 respuesta se puede utilizar para comunicar una petición para cancelar la transacción o marcar la transacción como fraudulenta, Por ejemplo. En tales situaciones, el sistema de autorización 20 comunica el hecho de que la transacción puede ser fraudulenta al

sistema de institución 10, que a su vez permitirá a la institución 50 tomar las acciones apropiadas para cesar la transacción y detener la transferencia de fondos.

Se prefiere que la ID de cliente y la ID de dispositivo se almacenen por el sistema de autorización 20 en una forma que las separe, por ejemplo por el uso de un algoritmo encriptado. Esto es para asegurar que el caso improbable de un ataque sobre el sistema de autorización fuera exitoso; el atacante no podría correlacionar la ID de cliente y la ID de dispositivo, y posteriormente imitar la autorización de una transacción fraudulenta. En una forma la ID de cliente se almacena de manera separada en un subconjunto de triple cortafuegos dentro del ambiente del sistema de autorización 20.

También se prefiere que la ID de cliente no se almacene o copie en cualquier parte durante el proceso de autorización de transacción. Esto puede requerir la facilitación de un pase en el sistema IVR 28 opuesto a un método de almacenamiento y validación.

De acuerdo con una modalidad particularmente preferida, se proporciona un sistema de pago remoto 100 que incorpora el sistema de actualización.

La funcionalidad y el uso de una implementación del sistema 100 se ilustran en las Figs. 6 a 13. El sistema de paga remoto 100 permite a un cliente 40 transar pagos por bienes y servicios de manera remota de una forma segura con los miembros 60 del sistema 100. La implementación preferida del sistema 100, de acuerdo con el cual los usos del sistema 100 se ilustran en las Figs 6 a 13, incluye por lo menos unos medios de almacenamiento de datos 70 para contener datos actualizable que se relacionan con cada cliente 40, y cada miembro 60 del sistema 100, en donde cada cliente 40 tiene por lo menos un perfil de registro asociado 80 con una reserva monetaria relacionada 90.

El sistema 100 también incluye una arquitectura de procesamiento de datos 110 que tiene por lo menos unos medios de procesamiento de datos 120 y un sistema de caja de compensación 125 para liquidar endeudamiento entre los miembros 60 y los clientes 40 del sistema 100, en por lo menos unos medios de comunicación 130 asociados con la arquitectura de procesamiento de datos 110 para comunicar con un cliente 40, y por lo menos un dispositivo de comunicación remoto 30 mantenido por cada cliente 40 para comunicar con los medios de comunicación 130.

El cliente 40 utiliza el sistema 100 para transar pagos 140 por bienes y servicios conforme a la petición de pago 150, la petición de pago 150 activa un evento de comunicaciones 165 de por lo menos unos medios de comunicación 130 a por lo menos un dispositivo de comunicación remoto 30 con el propósito de validar la identidad del cliente 40 y tener acceso al perfil de registro respectivo 80, y una vez se ha validado la identidad del cliente 40, permite al cliente 40 transar pagos 140 suministra un balance positivo que permanece en la reserva monetaria 90.

Típicamente habrá por lo menos dos categorías de membresías del sistema, a saber miembros de negocios 60 y miembros cliente 40. Habrá típicamente una pluralidad de miembros en cada categoría de membresía. La membresía de la categoría de miembro de negocio 60 se puede controlar estrictamente y/o limitar por el administrador del sistema 160. La membresía de la categoría de miembro cliente 40 se puede proporcionar después de un proceso de solicitud que se puede someter a aprobación por el administrador 160. De manera importante, los miembros de negocios 60 del sistema 100 también pueden ser miembros cliente 40 del sistema 100.

El administrador del sistema 160 ofrecerá típicamente membresía al miembro de negocio 60 y a los miembros cliente. La membresía puede requerir una suscripción. Los

miembros de negocios 60 pueden pagar generalmente una tarifa de suscripción anual que les permitirá acceso al sistema 100. Los miembros de negocios 60 pueden estar provistos con un único número de identificación y clave para propósito de identificación. Los miembros de negocios 60 pueden recibir boletines regulares y actualización acerca del sistema 100, así como también los resultados de análisis de datos desarrollados sobre la información que se relaciona con el sistema 100. Estos boletines se pueden preparar por el administrador del sistema 160. Típicamente, la información tal como ésta relacionará el programa y sus beneficios, publicidad del programa o similares. El administrado del sistema 160 puede compilar una base de datos 160 que contiene los detalles de los miembros de negocios 60 y cualquier otra información o estadística que desee el administrador del sistema 160.

El miembro de negocios 60 puede recolectar y/o actualizar información sobre los miembros de cliente 40 del programa que utiliza el sistema 100 para pagar bienes o servicios de los miembros de negocios 60. Esta información se puede comunicar al administrador del sistema 160 y se puede almacenar sobre la base de datos de cliente 70.

Puede haber preferiblemente dos porciones o sectores del sistema. Las dos porciones del sistema se pueden conocer preferiblemente como el extremo frontal y el extremo trasero. El extremo frontal puede comprender preferiblemente una interfaz de usuario. La interfaz de usuario permite a un suscriptor o administrador de base de datos tener acceso o conectarse al extremo trasero del sistema 100. El extremo delantero o la interfaz de usuario se puede ubicar preferiblemente o de manera accesible utilizando un explorador de Internet o teléfono móvil, PDA u otro dispositivo personal con capacidad de comunicación. Alternativamente la interfaz de usuario se puede ubicar sobre un

computador o servidor o sobre una red de computadores o servidores. Esta puede ser de cualquier configuración o tipo adecuado.

El extremo trasero del sistema 100 puede preferiblemente incluir por lo menos
5 unos medios de almacenamiento de datos típicamente una pluralidad de base de datos. Por lo menos una de las base de datos puede preferiblemente ser una base de datos de clientes 70, que contiene información acerca de lo clientes 40 y su registro monetario asociado 90, y la segunda base de datos puede preferiblemente ser una base de datos de miembros de negocios 170, que contiene información acerca de los miembros de
10 negocios 60 y sus cuentas 180. El acceso a cada base de datos por vía de la interfaz de usuario puede ser preferiblemente diferenciado dependiendo del acceso o detalles de registro. Por ejemplo el acceso por un cliente 40 puede permitir que solo se desarrolle funciones restringidas o particulares, que se pueden restringir en una forma similar al acceso otorgado a los miembros cliente 40 pero con igual o diferente funcionalidad
15 mientras que el acceso por el administrador del sistema 160 puede otorgar estatus de "superusuario" y permitir acceso a todas las porciones del sistema 100 y a todas las funciones del sistema 100.

Típicamente un miembro potencial puede tener contacto con el administrador del
20 sistema 160 con el fin de suscribirse al sistema 100. El administrador del sistema puede proporcionar de manera adecuada al miembro con un único nombre de usuario y clave para permitir acceso al sistema. El miembro puede pagar preferiblemente al administrador del sistema 160 una tarifa de suscripción con el fin de tener acceso al sistema 100 durante un periodo de tiempo preestablecido. El nombre de usuario y la
25 clave puede incluir un Número de Identificación Personal, un número de cuenta, o el nombre de usuario puede estar ligado a las características de identificación de los medios de comunicación remoto utilizados y las características de identificación de los

medios de comunicación remoto particulares por el cliente 40 pueden diferir de acuerdo con el tipo de dispositivo 30 utilizado. Por ejemplo, los computadores que utilizan conexiones a Internet cableadas pueden utilizar medios ID tal como Tecnología de Identificación de Llamada (CLI), servicio de telefonía móvil pueden permitir características de identificación de tarjeta SIM a ser utilizadas y acceso a Internet directo a la interfaz puede utilizar la dirección de red o la dirección del protocolo de Internet, validado preferiblemente a través de un proveedor de servicios como un nombre de usuario.

La anterior discusión se basa acerca de una telefonía móvil o dispositivo de cómputo. El sistema 100 también se puede utilizar sobre el Internet por ejemplo. Luego de abrir la página de la red predeterminada, el cliente 40 se le puede preguntar de manera adecuada que ingrese su nombre de usuario y clave con el fin de tener acceso al sistema 100. La entrada correcta de un nombre de usuario de cliente 40 y la clave acompañante puede preferiblemente permitir acceso al sistema 100 como un cliente 40.

Uso del sistema 100 por miembros de negocios 60 puede ser ligeramente diferente a aquel de los miembros de cliente 40. Los miembros de negocios 60 utilizarán preferiblemente el sistema 100 para notificar a los clientes 40 de los requerimientos de pagos pendientes 150 y monitorear su propia cuenta de balance 180. El sistema 100 también puede permitir al un miembro de negocios 60 producir registros estadísticos de cuentas del sistema de información 100.

El uso del sistema 100 por el administrador del sistema 160 también puede preferiblemente ser accesado a través del extremo frontal de la interfaz de usuario. En una forma similar a una entrada de cliente 40 de su nombre de usuarios y clave, el administrador 160 también puede tener un nombre de usuario y clave, la entrada puede

permitir de manera adecuada acceso más amplio o no restringido al sistema 100 que aquel permitido a un cliente 40.

La entrada correcta del nombre de usuario del administrador 160 y la clave
acompañante puede permitir preferiblemente acceso al sistema 100 como el
administrador de base de datos. El administrador 160 tendrá preferiblemente la
capacidad de mantener el sistema 100, que incluye corregir los perfiles de registro de
cliente 80 y las billeteras virtuales 90 para corregir errores y también generar informes
del sistema 100.

Los clientes 40 pueden tener la opción para actualizar sus detalles de
identificación o detalles de contacto por vía, por ejemplo, de una interfaz de red. Luego
de seleccionar la opción para modificar los detalles del cliente 40, se muestra
preferiblemente un formulario editable que permite al cliente 40 editar sus detalles de
cuenta. Esto puede permitir la modificación de los detalles tal como el nombre de
usuario, clave, nombre de contacto y detalles de dirección que incluyen números de
telecomunicaciones, correo electrónico y dirección de sitio de red del cliente. El cambio
de información de identificación de esta manera activará típicamente el proceso de
autenticación a ser llevado a cabo de nuevo.

Las características específicas preferidas del sistema 100 se describen más
fácilmente con respecto al uso del sistema 100 por un cliente 40 o miembro de negocio
60, o por el administrador 160.

La primera etapa en el sistema 100 generalmente será establecer un nuevo perfil
de registro 80 de cliente 40. Los eventos que pueden iniciar un nuevo Registro de
Cliente junto con un proceso preferido para distribución con los eventos se identifica en

la Fig. 7. El extremo frontal del sistema se puede alcanzar preferiblemente utilizando un explorador de Internet para visitar una dirección de sitio de red predeterminada. Esto se puede desarrollar por el cliente 40 directamente utilizando la interfaz de Internet o al poner en contacto un funcionario de servicio al cliente (CSO) del sistema 100 por otros medios y el CSO utiliza la interfaz de Internet para ingresar los detalles del cliente 40 requeridos para la validación inicial del cliente 40. La implementación preferida del proceso actual del nuevo Registro de Clientes se ilustra en la Fig. 8.

Luego de seleccionar la opción para ingresar los detalles de cliente 40, se exhibe preferiblemente un formulario editable que permite al cliente 40 (o CSO) ingresar (o editar) sus detalles de suscripción o detalles de cuenta. Esta puede permitir la modificación de los detalles tal como nombre de usuario, clave, nombre de contacto y detalles de dirección que incluyen números de telecomunicaciones, correo electrónico y dirección de sitio de red del cliente 40. esta también puede incluir otros datos de fondo tal como fecha de nacimiento, detalles bancarios y de referencia, si existe cualquier información de identificación ingresada que ya este en uso o sea pieza de información faltante, se puede publicar una pregunta para pedir la información o corrección de la información.

Una vez se ha validado la información de identificación del cliente 40 por un procedimiento de validación principal, la información ingresada se puede utilizar para crear un perfil de registro 80 del cliente 40 y una reserva monetaria o "billetera virtual" 90.

Los fondos para usos en el sistema 100 de la presente invención se transfieren típicamente en la billetera virtual 90 del cliente 40. La transferencia de fondos puede ser de una cuenta débito 210 con un proveedor de servicio financiero establecido 190 tal

como un banco, sociedad constructora u otra o de una instalación crediticia ofrecida por un proveedor 190. Preferiblemente, en esta etapa, la fuente preferida para la transferencia se puede nominar por el cliente 40 pero no procesar.

5 Esto puede ser seguido por un segundo procedimiento de autenticación típicamente siguiendo un procedimiento de verificación secundario por el administrador del sistema 160 así como también una revisión rigurosa de la información suministrada que puede requerir confirmación de las partes independientes del administrador del sistema 160.

10

Una vez el cliente 40 informa al sistema 100 de la fuente preferida para la transferencia, entonces se le puede pedir al cliente 40 que siga un procedimiento de autenticación para autenticar su identidad, validar el acceso al sistema 100 y a la cuenta de fuente 210 para la transferencia o similar. Una implementación preferida del proceso
15 de autenticación se ilustra en la Fig. 9.

El procedimiento de autenticación puede incluir la arquitectura de procesamiento de datos 110 que crea una pregunta de autenticación y comunica la autenticación a por lo menos un medio de comunicación 130 asociados con la arquitectura de
20 procesamiento de datos 110. La validación y autorización para el pago 200 se desarrolla utilizando el sistema de autenticación 20 destacado anteriormente. De nuevo, se otorga autenticación o se declina, un mensaje adecuado informa al cliente 40 el resultado del proceso de autenticación que se generará preferiblemente por la arquitectura de procesamiento de datos 110 y se reenviará al dispositivo de
25 comunicación remoto preferido 30 del cliente 40 por vía de por lo menos unos medios de comunicación 130 asociados con la arquitectura de procesamiento de datos 110.

Si el proceso de autenticación es exitoso, se registra el pago 200 por el sistema 100 y la billetera virtual 90 del cliente 40 se actualiza a la cuenta para el pago 200 y refleja exactamente los fondos disponibles del cliente 40 a través del sistema 100.

5 También será posible típicamente una transferencia de fondos postinicio a la parte superior de su billetera virtual 90 o balance u otro tipo de transacción. Cada transacción se someterá típicamente al proceso de autenticación que incluye poner en contacto al cliente 40 por el sistema 100 y la petición para validar la información.

10 Una vez se ha validado la identidad del cliente 40, el cliente 40 preguntará típicamente para transferir los fondos de inicio en su billetera virtual 90 para uso bajo el sistema 110. En este caso, el cliente 40 seguirá típicamente un primer procedimiento de depósito, una implementación preferida que se ilustra en la Fig. 10. la transferencia de fondos puede diferir dependiendo de si el cliente 40 está utilizando una instalación
15 débito o crédito. Si se utiliza una instalación crédito, el sistema 100 puede funcionar sobre una base en tiempo real, bajando la información de tarjeta de crédito y procesando el pago de tarjeta de crédito en demanda mientras que si se utiliza una instalación débito, el cliente 40 puede transferir fondos a su billetera virtual 90 para utilizar inmediatamente o en un momento posterior.

20

Luego de la pregunta para transferir fondos de inicio, el sistema 100 todavía utiliza el componente IVR 28 y generalmente en el mismo contacto como el contacto de autenticación, requerirá que el cliente 40 designe la cantidad a ser transferida. El sistema luego puede procesar esta petición con la institución financiera nominada 190
25 del cliente 40 y la cuenta y publicación de una notificación exitosa/no exitosa al cliente 40. El cliente 40 entra en contacto con el componente IVR 28 que puede ser finalizado en esa etapa o el sistema 100 puede preguntar si cualquier actividad adicional se puede

tomar por el cliente 40. Si la transferencia es exitosa, se registra el pago 200 por el sistema 100 y la billetera virtual 90 del cliente 40 actualiza la cuenta para el pago 200 y para reflejar exactamente los fondos disponibles para el cliente 40 a través del sistema 100.

5

Típicamente, para balancear la carga de procesamiento sobre el sistema 100, las transacciones del cliente 40 y las actualizaciones a la billetera virtuales respectivas 90 se pueden conducir en tiempo real pero la actualización de la transferencia de fondos al miembro de negocios 60 del sistema 100 puede ocurrir en periodos de calma en el sistema 100. La actualización de transferencia de fondos para miembros de negocios 60 puede ocurrir en "chorros" voluminosos en donde se puede transferir una única cantidad a un miembro de negocios 60 con la información apropiada para identificar el pagador cliente 40. La sincronización de los periodos de calma puede ocurrir en un momento particular en cada periodo, típicamente cada día, o el sistema 100 se puede automonitorear para procesar transferencias para negocios 60 cuando el procesamiento de la transferencia del cliente 40 cae.

Dependiendo del resultado del primer procedimiento de deposito, el perfil de registro 80 y más particularmente, la billetera virtual 90 del cliente 40 puede ser "cargada" con una entrada que indica el valor de los fondos transferidos de la cuenta fuente 210 en la billetera virtual 90 del cliente 40 que luego puede ser utilizada por el cliente 40 para hacer pagos 140 a los miembros de negocios 60 del sistema 100 en cualquier momento.

Una implementación preferida del proceso de pago se ilustra en la Fig. 11. con el fin de hacer un pago 140 utilizando el sistema, una petición de pago 150 se generará típicamente a través de una interfaz para el sistema 100 mediante un miembro de

negocios 60 (una operación de “halado”), un cliente 40 (una operación “de empuje”) o mediante otros medios y la petición de pago 150 se marcará preferiblemente y se asociará con un perfil de registro 80 del cliente 40 particular. El cliente 40 también se notificará de la petición de pago pendiente 150 por el miembro de negocios 60
5 directamente o por el sistema 100 en sí mismo.

Una vez la petición de pago 150 se ha generado, el cliente 40 indica que el pago 140 que utiliza el sistema 100 se desarrolla, normalmente por contacto con los medios de comunicación 130 asociados con la arquitectura de procesamiento de datos 120. La
10 arquitectura de procesamiento de datos 120 verifica típicamente los detalles de la petición de pago 150 y también puede verificar la identidad del cliente 40 y la disponibilidad de fondos en la billetera virtual del cliente 90 y luego reenviar una pregunta a los medios de comunicación 130 para poner en contacto al cliente 40 para la validación o autorización para el pago 140.

15

De nuevo, la validación y autorización para el pago 140 se desarrolla utilizando el sistema de autorización 20 destacado anteriormente. Una vez se otorga la autenticación o se rechaza, un mensaje adecuado informa al cliente 40 del resultado del proceso de autenticación que preferiblemente se generará por la arquitectura de procesamiento de
20 datos 120 y se reenviará al dispositivo de comunicaciones remoto 30 preferido del cliente por vía de por lo menos unos medios de comunicación 130 asociados con la arquitectura de procesamiento de datos 120.

Si el proceso de autenticación es exitoso, se registra el pago 140 por el sistema
25 100 y la billetera virtual 90 del cliente 40 actualiza la cuenta para el pago 140 y refleja exactamente los fondos disponibles para el cliente 40 a través del sistema 100.

Una transferencia de fondos post-inicio a la parte superior de su billetera virtual
90 (una implementación preferida de este proceso se ilustra en la Fig. 12) o balance
(una implementación de este proceso se ilustra en la Fig. 13) u otro tipo de transacción
también será típicamente posible. Cada transacción se someterá típicamente al proceso
5 de autenticación utilizando el sistema de autorización. Utilizando el sistema de
autorización 20 que incluye poner en contacto el cliente por el sistema 100 y la petición
para validar la información.

En la presente divulgación y reivindicaciones (si existe), la palabra “que
10 comprende” y sus derivados incluye “comprenden” y “comprende” incluye cada uno de
los enteros establecidos pero no excluye la inclusión de uno o más enteros adicionales.

La referencia a lo largo de esta divulgación a “una modalidad” o “una modalidad”
significa que una característica particular, estructura o rasgo descrito en relación con la
15 modalidad se incluyen en por lo menos una modalidad de la presente invención. Así, la
aparición de la frase “en una modalidad” o “una modalidad” en varios lugares a lo largo
de esta divulgación no necesariamente se refieren todos a la misma modalidad.
Adicionalmente, estas características, estructuras o rasgos particulares se pueden
combinar en cualquier forma adecuada en una o más combinaciones.

20

La anterior discusión se considera solo como ilustrativa de los principios de la
invención. Adicionalmente, en razón a que numerosos cambios y modificaciones
ocurrirán fácilmente a aquellos expertos en la técnica, no es deseable limitar la
invención a la construcción exacta y operación mostrada y descrita, y de acuerdo con lo
25 anterior, todas las modificaciones adecuadas y equivalentes se pueden reclasificar,
para que caigan dentro del alcance de la invención.

REIVINDICACIONES

1. Un sistema de autorización de transacción que permite a un cliente autorizar transacciones que se relacionan con por lo menos una cuenta de cliente asociada con una institución, el sistema incluye:

Medios de almacenamiento de datos para permitir acceso a

- (a) Datos de identificación asociados con el cliente;
- (b) Datos de identificación asociados con un dispositivo de comunicación remoto (RCD) del cliente;
- (c) Datos de identificador de seguridad que asocian por lo menos una cuenta de cliente con uno o ambos de (a) y (b);

Unos primeros medios de comunicación para permitir comunicación con el cliente por vía del RCD para autorizar una transacción sobre por lo menos una cuenta de cliente;

Una arquitectura de procesamiento de datos que incluye medios de procesamiento de datos para identificar el cliente utilizando (a), identificar el RCD utilizando (b) y determinar si la transacción se autoriza por el cliente; y

Un segundo medio de comunicación para recibir una petición de autorización en relación con la transacción y proporcionar una indicación a la institución de si o no la transacción se autoriza por el cliente,

en donde la petición de autorización recibida y la indicación prevista para la institución se relacionan con los datos de identificador de seguridad.

- 2. El sistema de autorización de transacción de la reivindicación 1, en donde los datos de identificador de seguridad no se comunican al cliente.
- 3. El sistema de autorización de transacción de la reivindicación 2, en donde los datos de identificador de seguridad no es el mismo que, ni se deriva de las características de o la información personal que se relaciona con el cliente.
- 4. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 3, en donde los primeros medios de comunicación permiten comunicación con el cliente por vía de RCD utilizando un medio de comunicación que es distinto de los medios de comunicaciones utilizados para conducir la transacción.
- 5. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 4, en donde los primeros medios de comunicación permiten comunicación con el cliente por vía de RCD utilizando dos o más sesiones de comunicación.
- 6. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 5, en donde (a) incluye uno o más de un PIN, una clave, frase de paso o datos biométricos.
- 7. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 6, en donde (b) incluye uno o más de un número telefónico, una identidad de equipo móvil internacional (IMEI), dirección de protocolo de Internet (IP), o dirección de control de acceso de medio (MAC).

8. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 7 en donde los primeros medios de comunicación incluyen un sistema de respuesta de voz interactivo (IVR).

5 9. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 8, en donde los medios de almacenamiento de datos permiten adicionalmente acceso a la información de contacto RCD para uso por los primeros medios de comunicación para permitir comunicación con el cliente por vía RCD.

10

10. Un método para permitir a un cliente autorizar transacciones que se relacionan con por lo menos una cuenta de cliente mantenida en una institución, el método incluye las etapas de:

15

a) Un servidor de autorización que recibe una petición de autorización de la institución en relación con una transacción en por lo menos una cuenta de cliente.

20

b) La comunicación del servidor de autorización con el cliente por vía de un dispositivo de comunicación remoto (RCD) del cliente para autorizar la transacción.

25

c) El servidor de autorización que identifica el cliente utilizando datos de identificación asociados con el cliente al cual el servidor de autorización tiene acceso;

d) El servidor de autorización que identifica el RCD utilizando datos de identificación almacenados asociados con RCD para el cual el servidor de autorización tiene acceso;

5 e) El servidor de autorización que determina si se autoriza la transacción por el cliente;

f) El servidor de autorización comunica una indicación a la institución de si o no la transacción se ^{12a} autoriza por el cliente.

10 en donde la petición de autorización recibida por el servidor de autorización y la indicación proporcionada a la institución se relacionan por la institución y el servidor de autenticación con los datos de identificador de seguridad para asociar por lo menos una cuenta de cliente con una o ambos de los datos de
15 identificación almacenados asociados con el cliente y los datos de identificación almacenados asociados con el RCD.

11. El método de autorización de transacción de la reivindicación 10, en donde los datos de identificador de seguridad no se comunican al cliente.

20 12. El método de autorización de transacción de la reivindicación 10 o 11, en donde los datos de identificador de seguridad no con los mismos que, ni se derivan de, las características de o la información personal que se relacionan con el cliente.

25 13. El método de autorización de transacción de una cualquiera de las reivindicaciones 10 a 12, en donde la comunicación con el cliente por vía del

RCD utiliza un medio de comunicación que es distinto de los medios de comunicación utilizados para conducir la transacción.

14. El método de autorización de transacción de una cualquiera de las reivindicaciones 10 a 13, en donde la comunicación con el cliente por vía del RCD utiliza dos o más sesiones de comunicación.

15. El método de autorización de transacción de una cualquiera de las reivindicaciones 10 a 14, en donde los datos de identificación almacenados asociados con el cliente incluyen uno o más de un PIN, un clave, frase de paso, o datos biométricos.

16. El método de autorización de transacción de una cualquiera de las reivindicaciones 10 a 15, en donde los datos de identificación almacenados con el RCD incluyen uno o más de un número de teléfono, una identidad de equipo móvil internacional (IMEI), dirección de protocolo de Internet (IP) o dirección de control de acceso de medio (MAC).

17. El método de autorización de transacción de una cualquiera de las reivindicaciones 10 a 16, en donde la comunicación con el cliente por vía RCD incluye el uso de un sistema de respuesta de voz interactivo (IVR).

18. El método de autorización de transacción de una cualquiera de las reivindicaciones 10 a 17, en donde la comunicación con el cliente por vía de RCD se permite utilizando información de contacto RCD almacenada.

19. Un sistema de pago remoto que permite a un cliente transar pagos por bienes y servicios de manera remota en una forma segura con miembros del sistema, el sistema incluye:

- 5 i) Medios de almacenamiento de datos que contienen datos actualizables que se relacionan con cada uno de una pluralidad de clientes y cada uno de una pluralidad de miembros del sistema, en donde cada cliente tiene por lo menos un perfil de registro asociado con una reserva monetaria relacionada;
- 10 ii) Una arquitectura de procesamiento de datos que incluye medios de procesamiento de datos y un sistema de caja de compensación para liquidar endeudamiento entre los miembros y clientes del sistema,
- 15 iii) Medios de comunicación asociados con la arquitectura de procesamiento de datos para comunicar con los cliente por vía de un dispositivo de comunicaciones remoto (RCD) de cada uno de los clientes,

El sistema está dispuesto para que uno o más de dichos cliente transe pagos por bienes o servicios conforme a una petición de pago hecha por uno o más de los miembros, la petición de pago activa un evento de comunicaciones de los medios de comunicaciones al RCD del cliente relevante para el propósito de validar la identidad del cliente y tener acceso al perfil de registro respectivo, y el sistema está dispuesto adicionalmente con el fin de validar la identidad del cliente y una vez esto ha tenido lugar, permitir al cliente transar pagos dado un balance positivo que permanece en la reserva monetaria.

20. Un método de pago remoto que permite a un cliente transar pagos por bienes y servicios de manera remota en una forma segura con miembros de un sistema de pago remoto, el sistema incluye:

- 5 i) Medios de almacenamiento de pagos para contener datos actualizables que se relacionan con cada uno de una pluralidad de clientes, y cada uno de una pluralidad de miembros del sistema, en donde cada cliente tiene por lo menos un perfil de registro asociado con una reserva monetaria relacionada;
- 10 ii) Una arquitectura de procesamiento de datos que incluye medios de procesamiento de datos y un sistema de caja de compensación para liquidar endeudamiento entre los miembros y clientes del sistema,
- 15 iii) Medios de comunicación asociados con la arquitectura de procesamiento de datos para comunicación con los clientes por vía de un dispositivo de comunicaciones remoto (RCD) de cada uno de los clientes,
- 20 en donde el cliente utiliza el sistema para transar pagos por bienes o servicios conforme a una petición de pago hecha por uno o más de los miembros, el sistema de pagos activa un evento de comunicaciones de por lo menos unos medios de comunicaciones al RCD del cliente relevante para los propósitos de validar la identidad del cliente y tener acceso al perfil de registro respectivo, y una vez se ha validado la identidad del cliente se le permite al cliente transar pagos proporcionando un balance positivo que permanece en la reserva
- 25 monetaria.

21. Un sistema de pago remoto que permite a un cliente transar pagos por bienes y servicios de manera remota en una forma segura con miembros del sistema que incluye un sistema de autorización de transacción de acuerdo con una cualquiera de las reivindicaciones 1 a 9.

5

22. El sistema de autorización de transacción de una cualquiera de las reivindicaciones 1 a 9 para uso en el contexto de autenticación de transacciones de tarjeta de crédito.

10

23. El sistema de autorización de transacción sustancialmente como se describe aquí con referencia a una cualquiera de las modalidades de la invención ilustrada en los dibujos acompañantes.

15

24. Un método para permitir a un cliente autorizar transacciones sustancialmente como se describe aquí con referencia a una cualquiera de las modalidades de la invención ilustradas en los dibujos acompañantes.

20

25. Un sistema de pago remoto y métodos sustancialmente como se describe aquí con referencia a una cualquiera de las modalidades de la invención ilustradas en los dibujos acompañantes.

SISTEMA Y MÉTODO PARA AUTORIZACIÓN DE TRANSACCIÓN

RESUMEN

5 Un sistema de autorización de transacción (20) para permitir a un cliente (40) autorizar transacciones que se relacionan con por lo menos una cuenta de cliente (40) asociado con una institución (50), el sistema (20) incluye medios de almacenamiento de datos (24) para permitir acceso a datos de identificación asociados con el cliente (40) y un dispositivo de comunicación remoto (RCD) (30) del cliente (40), y datos de
10 identificador de seguridad que se asocian con la cuenta del cliente (40) con los datos de identificación. El sistema (20) también incluye medios de comunicación (26) para recibir una solicitud de autorización, que se relaciona con los datos de identificador de seguridad, en relación con la transacción desde la institución (50) y para permitir la comunicación con el cliente (40) por vía del RCD (30) para autorizar una transacción
15 sobre la cuenta de cliente (40). Los medios de procesamiento de datos (22) del sistema (20) identifican el cliente (40) y el RCD (30) utilizando los datos de identificación y determina si la transacción se autoriza por el cliente (40). Los medios de comunicación (26) proporcionan una indicación, que se relaciona con los datos de identificador de seguridad, con la institución (50) de si o no se autoriza la transacción por el cliente (40).

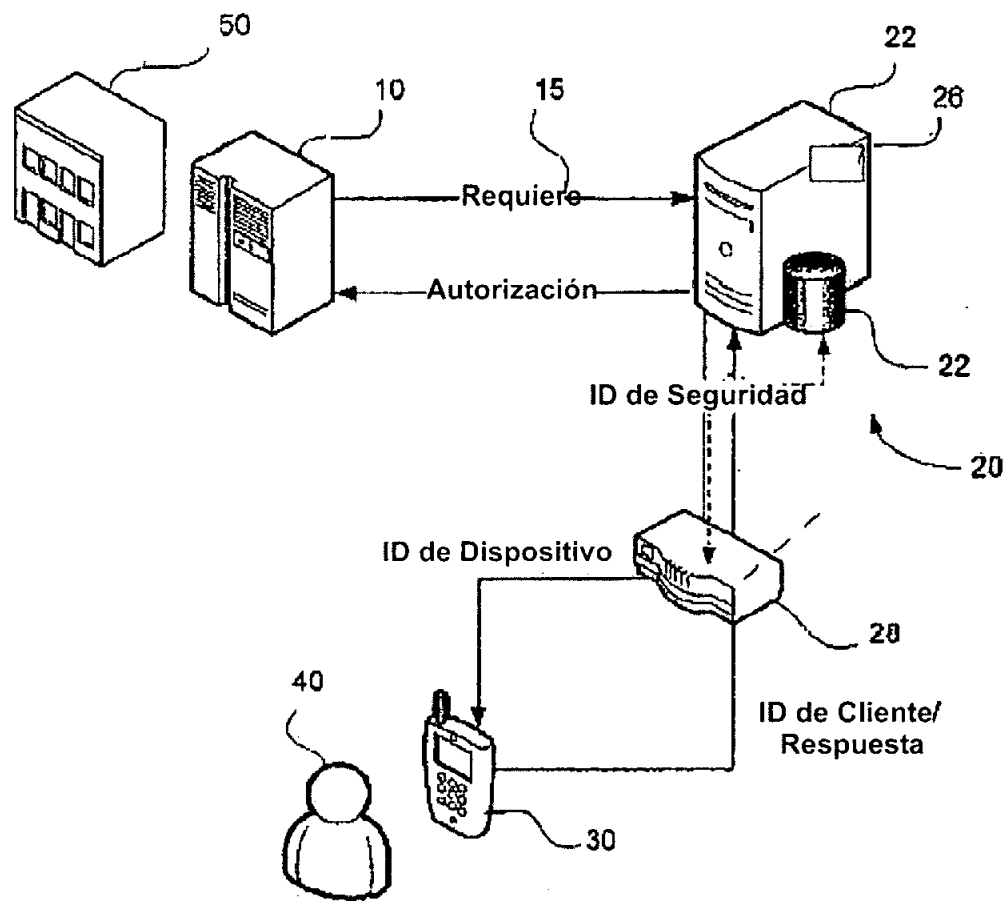


Fig. 1

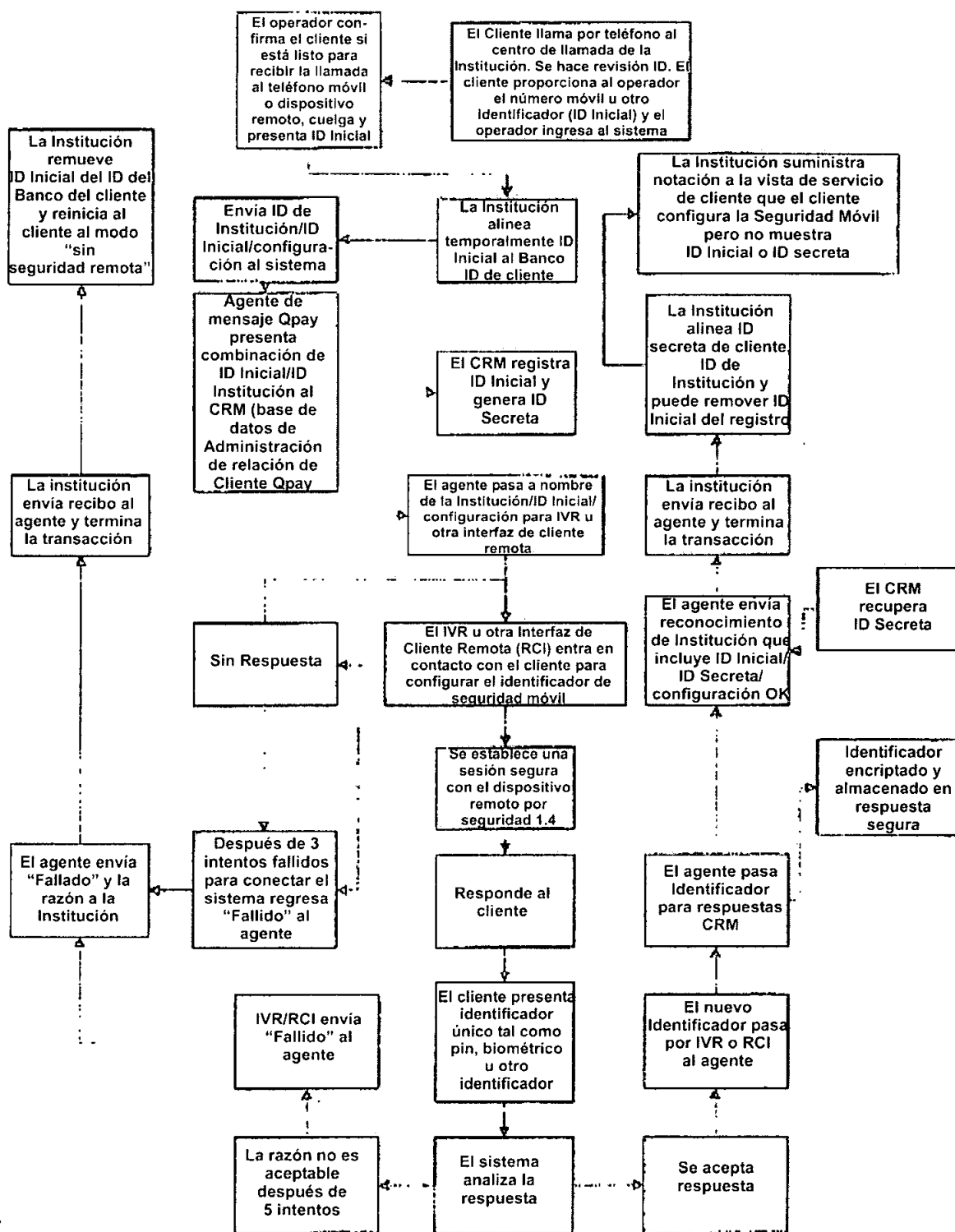


Fig. 2

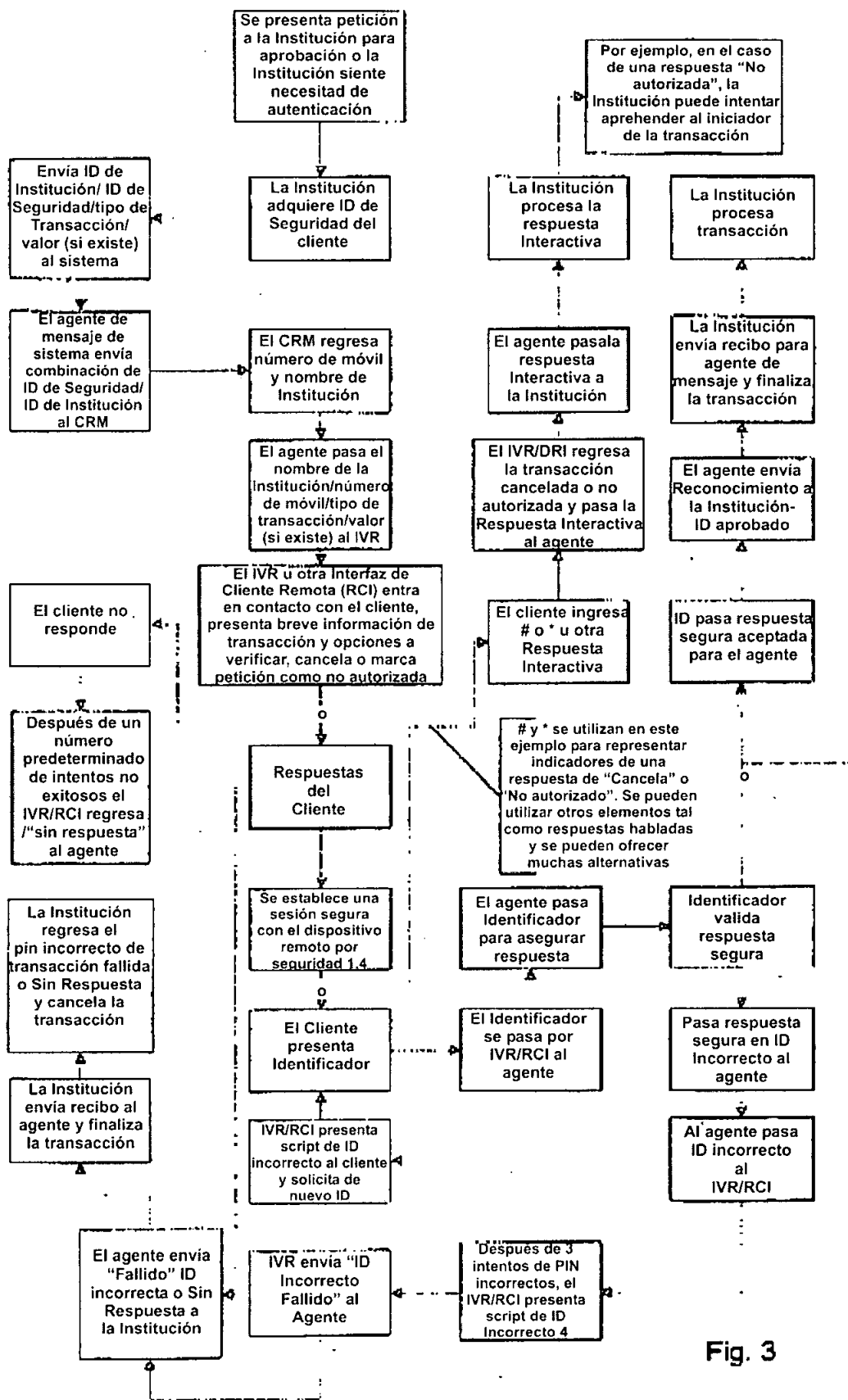


Fig. 3

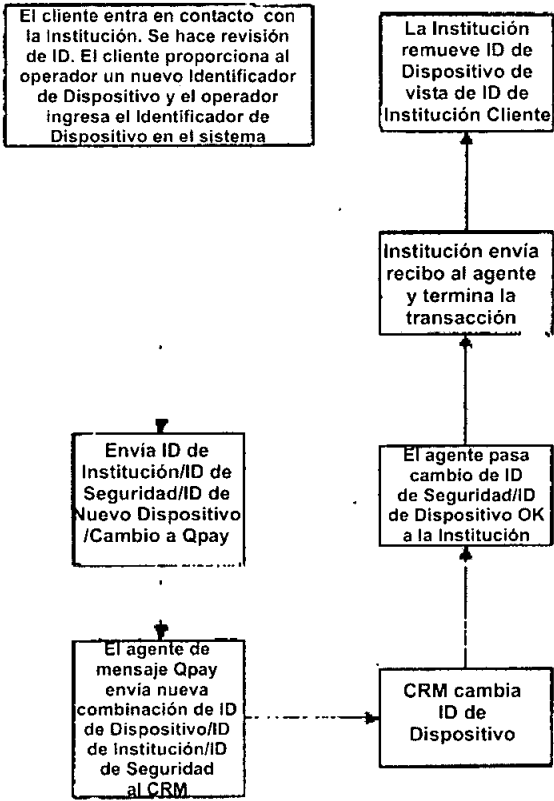


Fig. 4

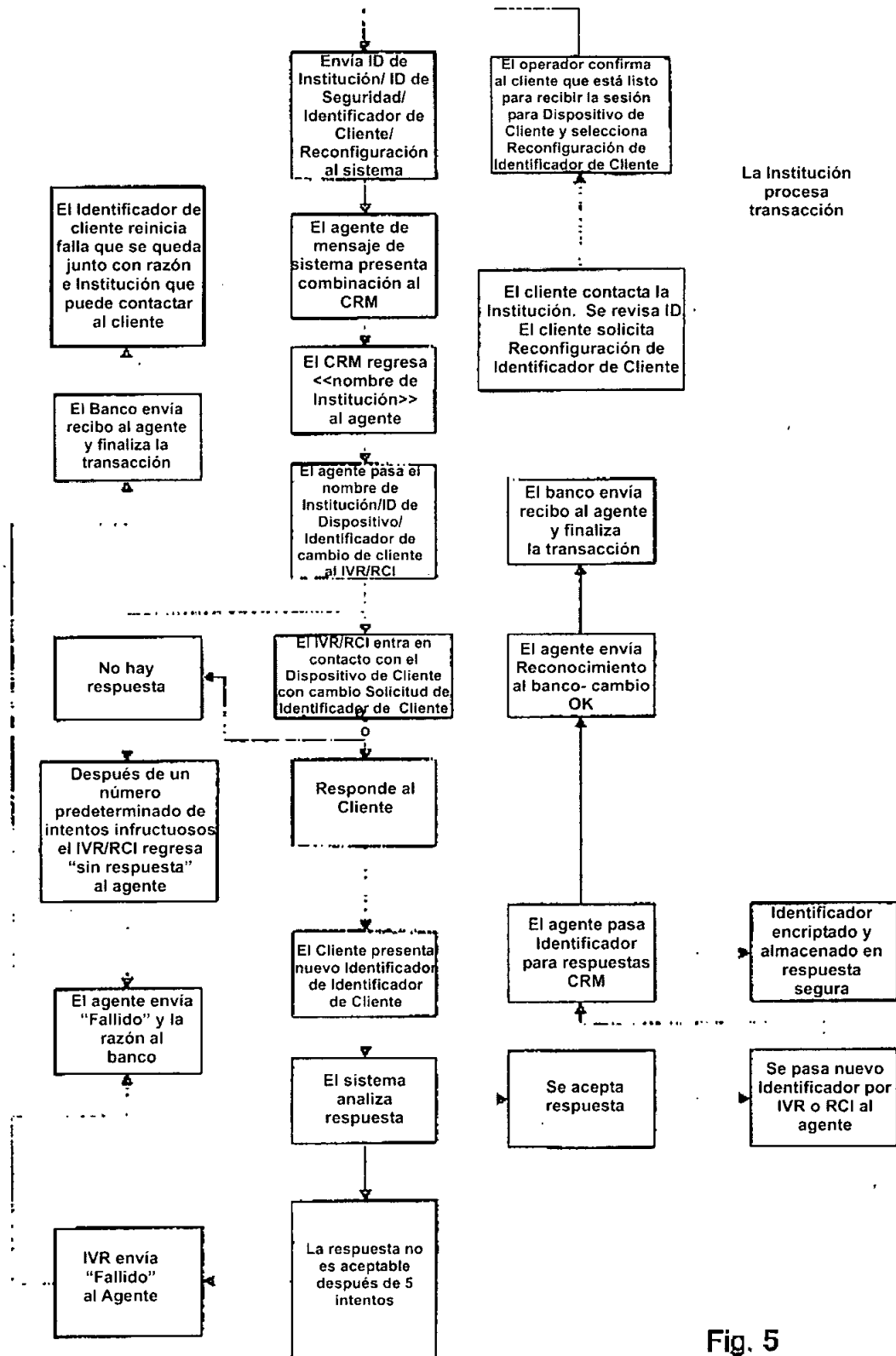


Fig. 5

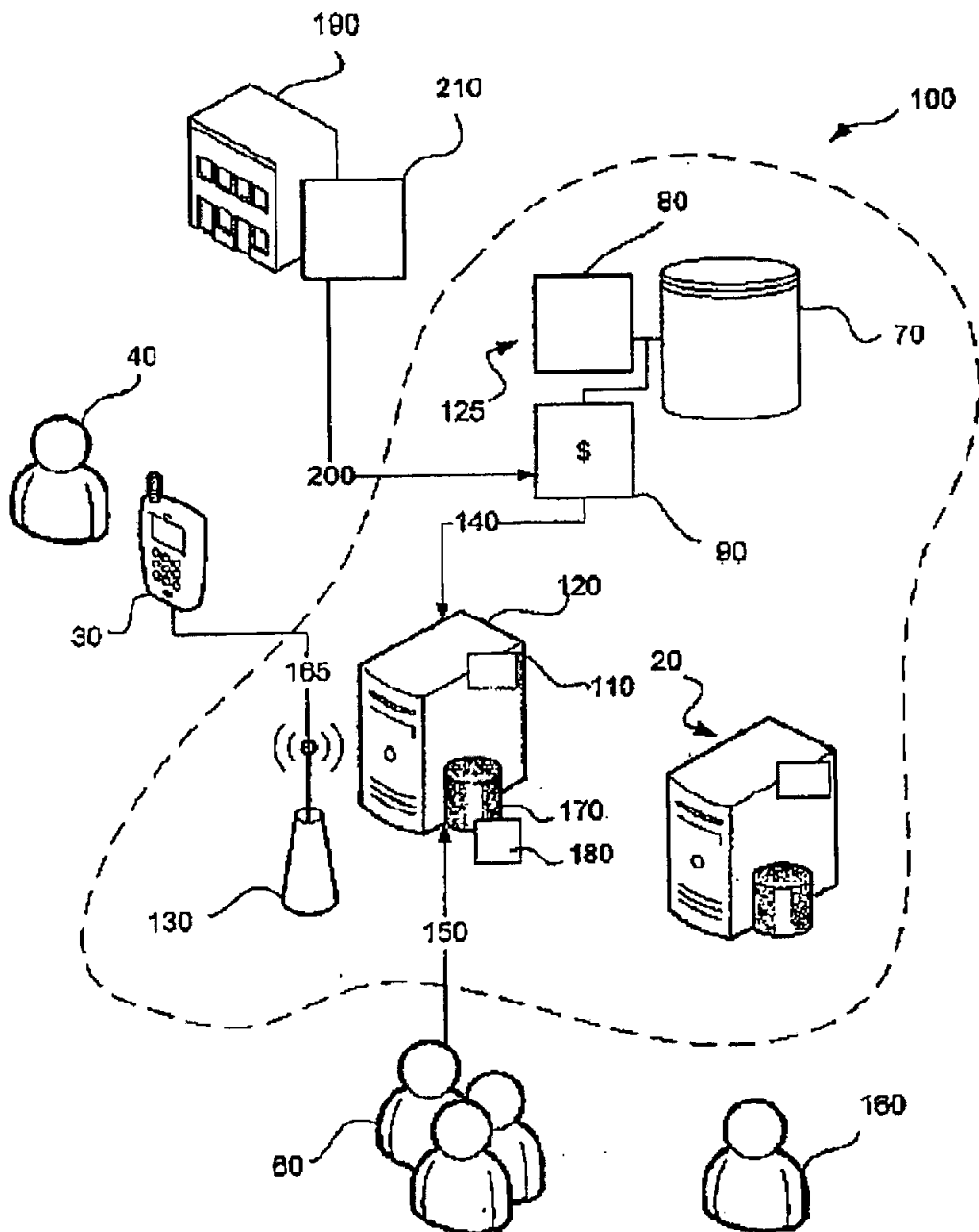


Fig. 6

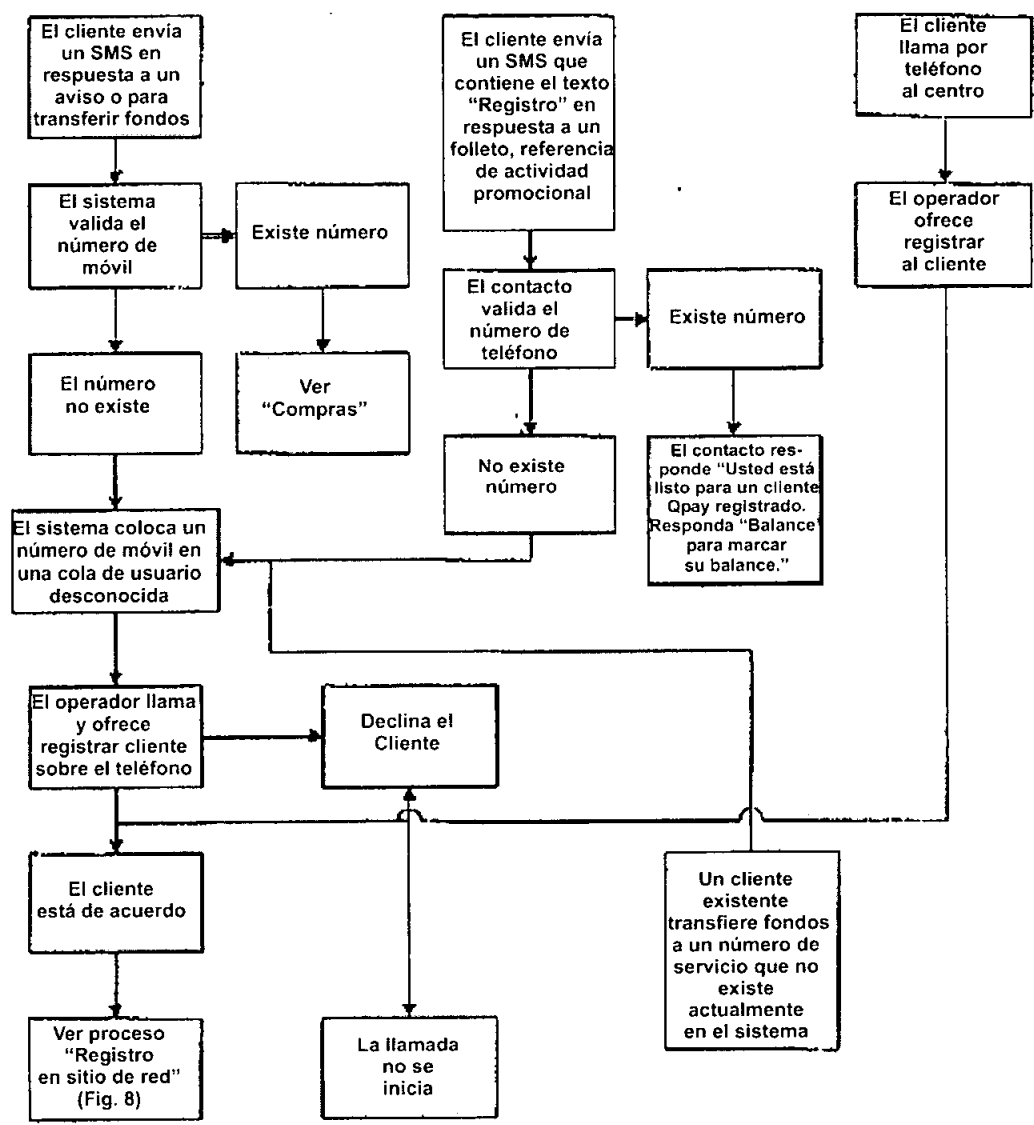


Fig. 7

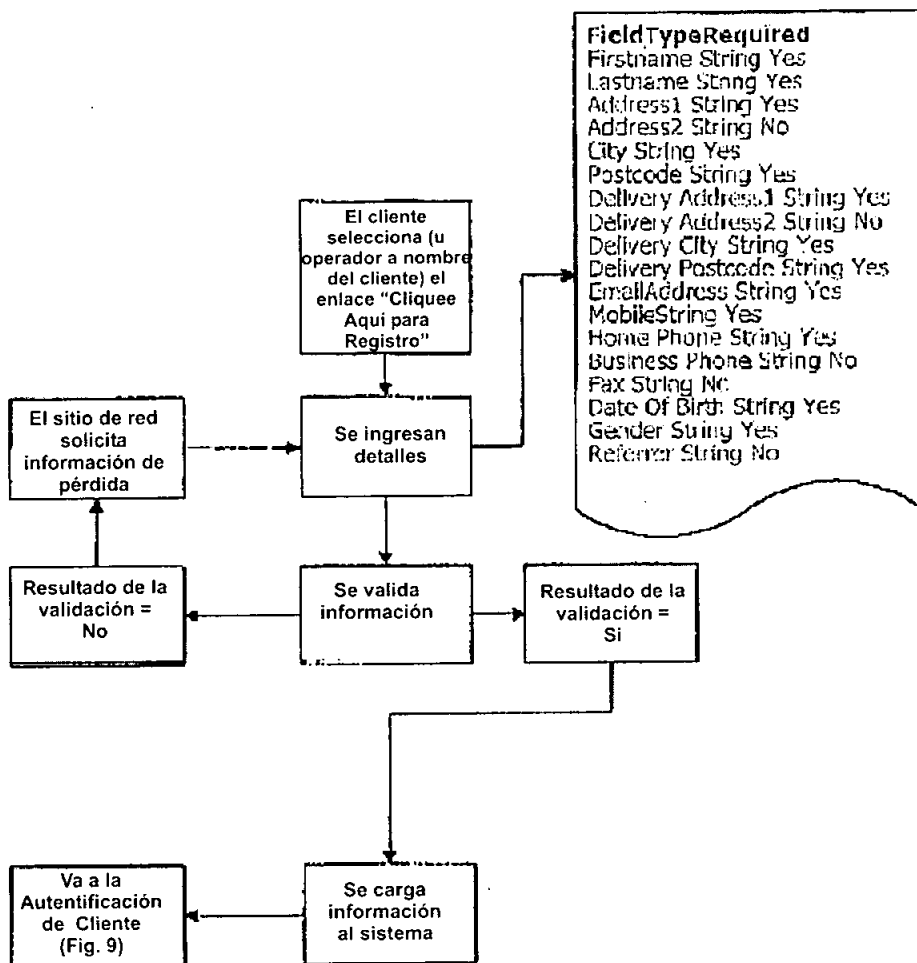


Fig. 8

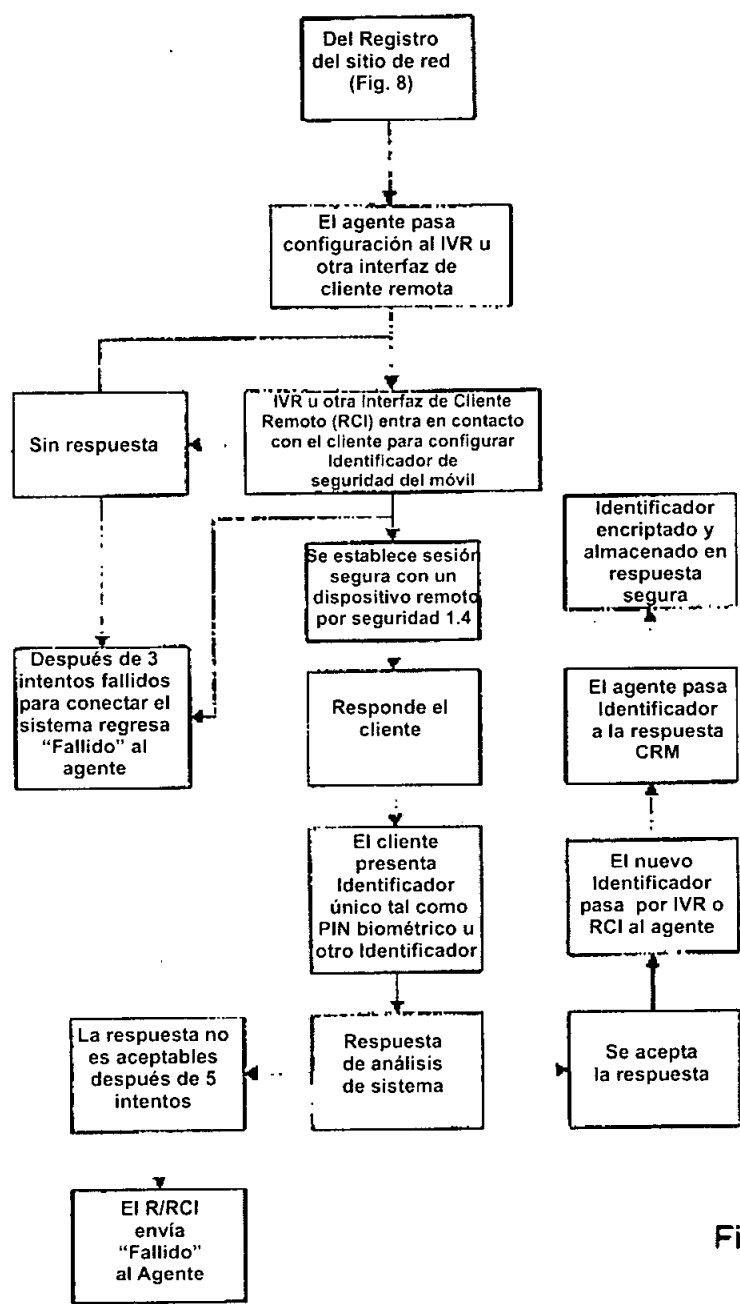


Fig. 9

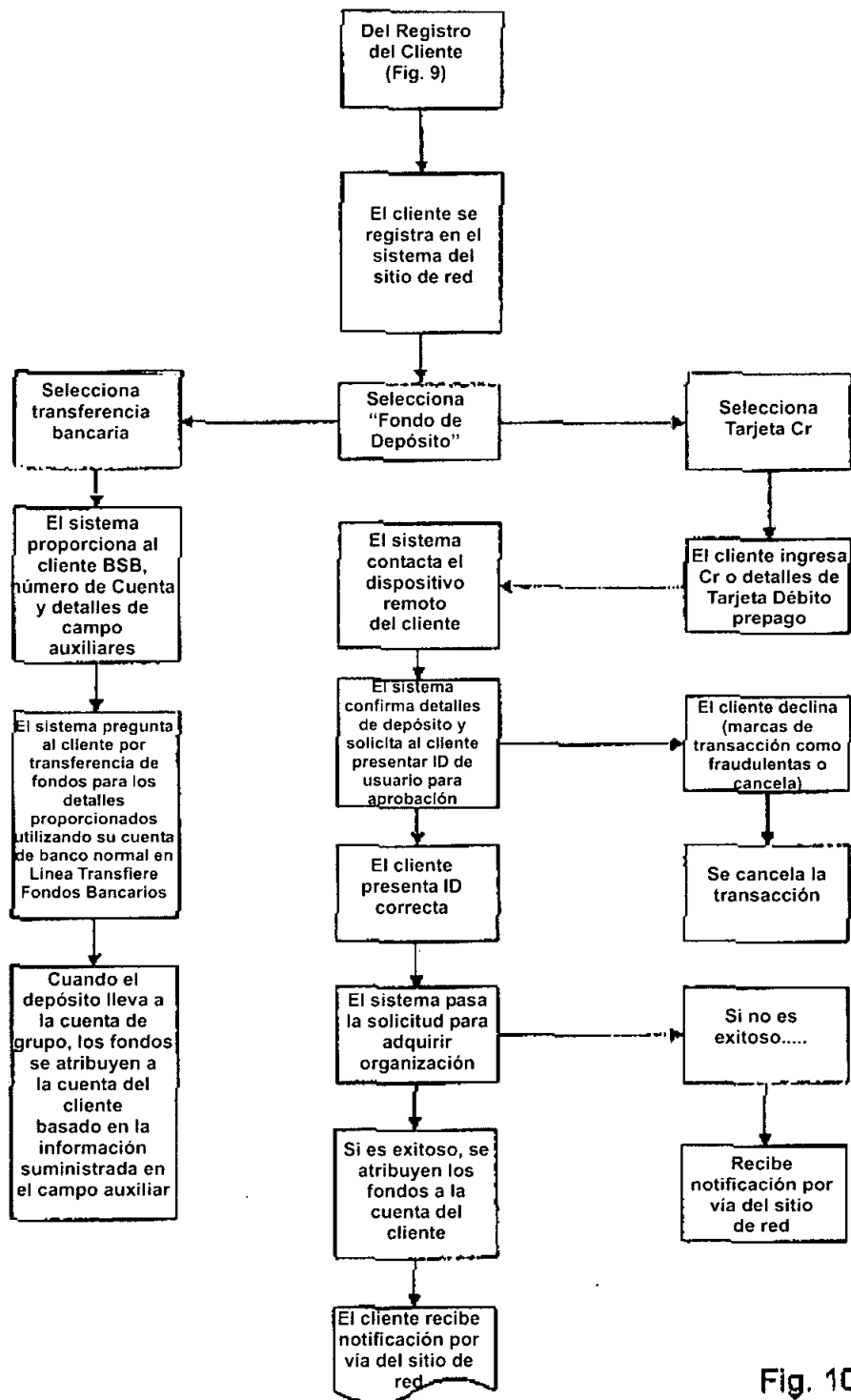
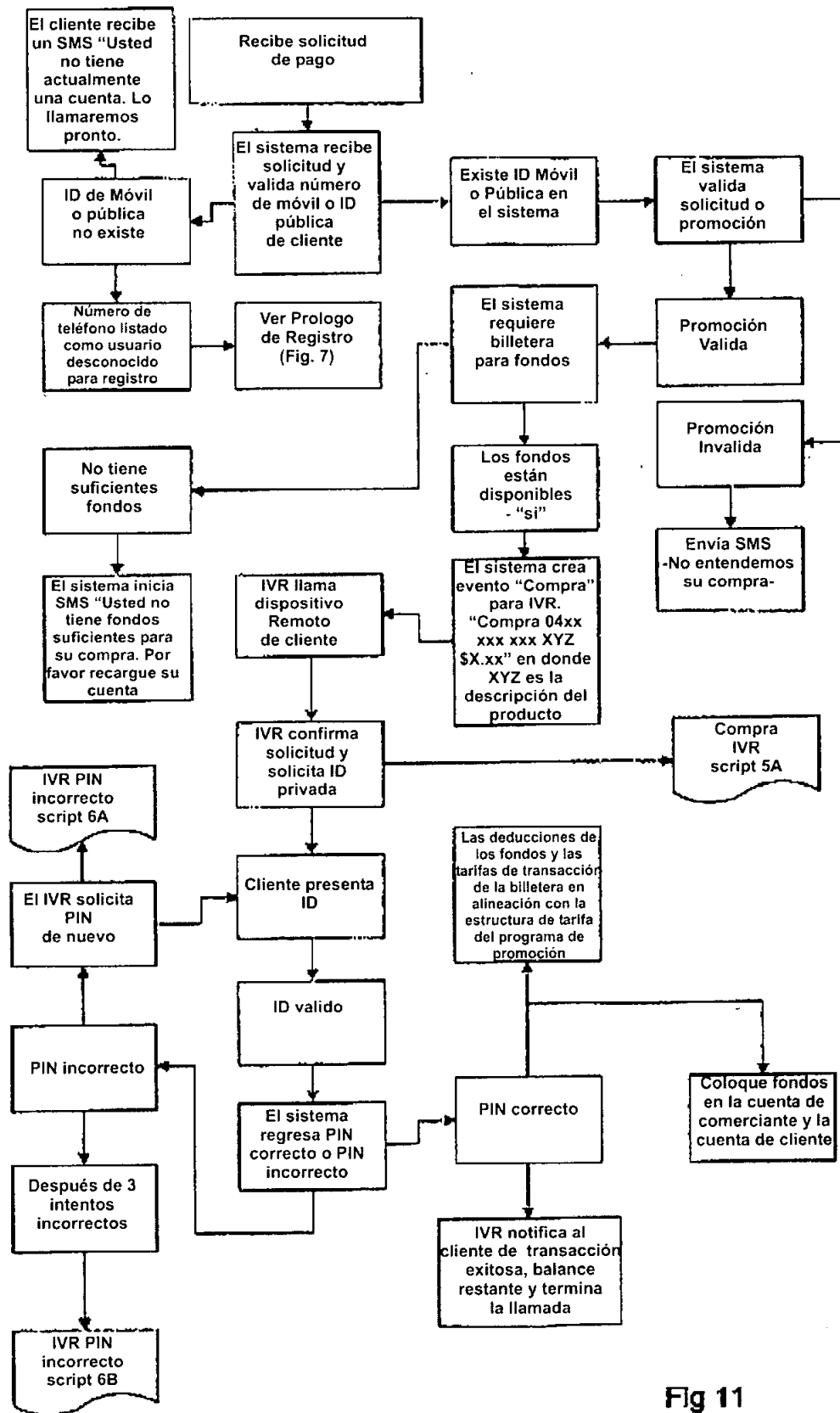


Fig. 10



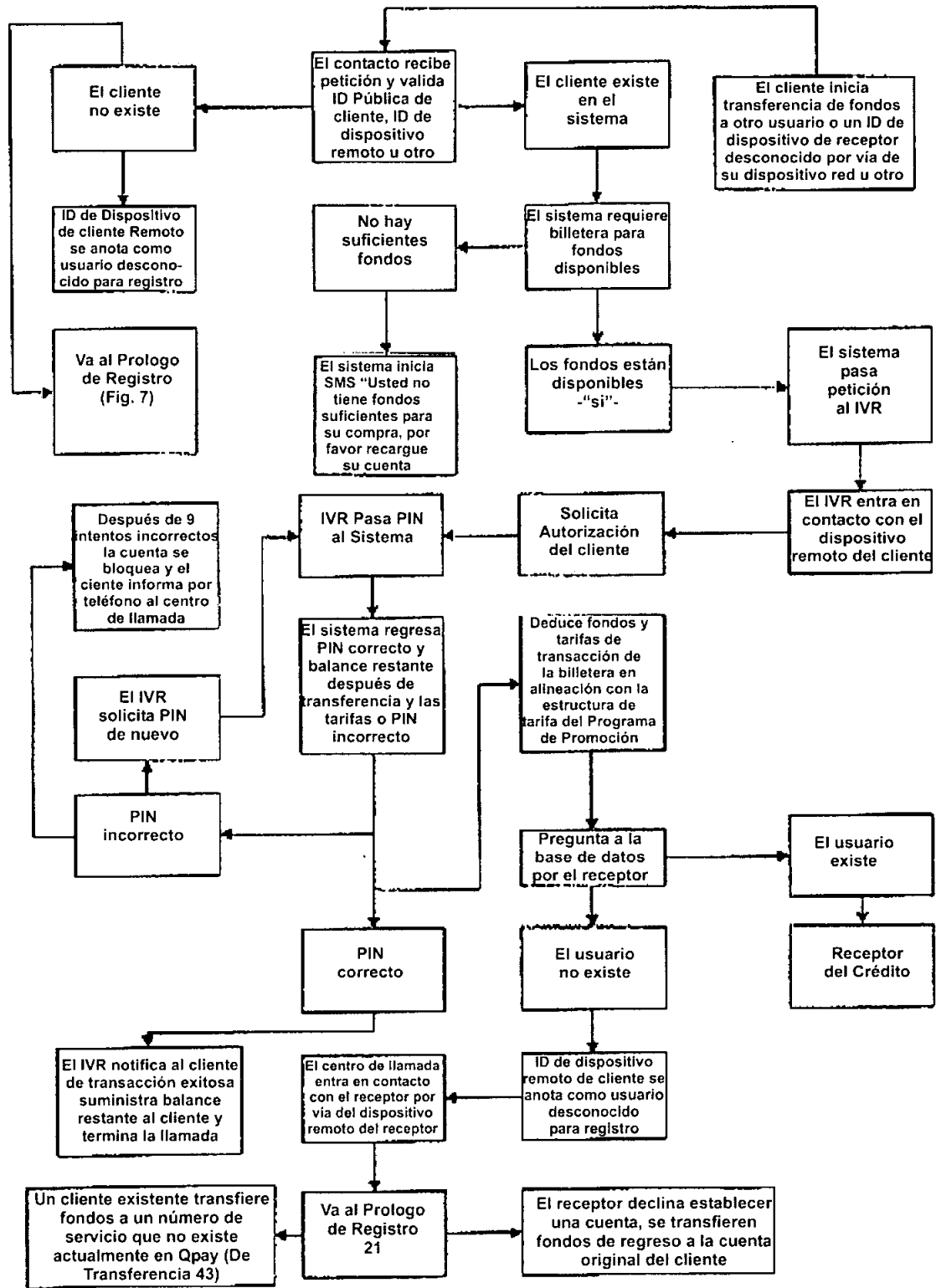


Fig 12

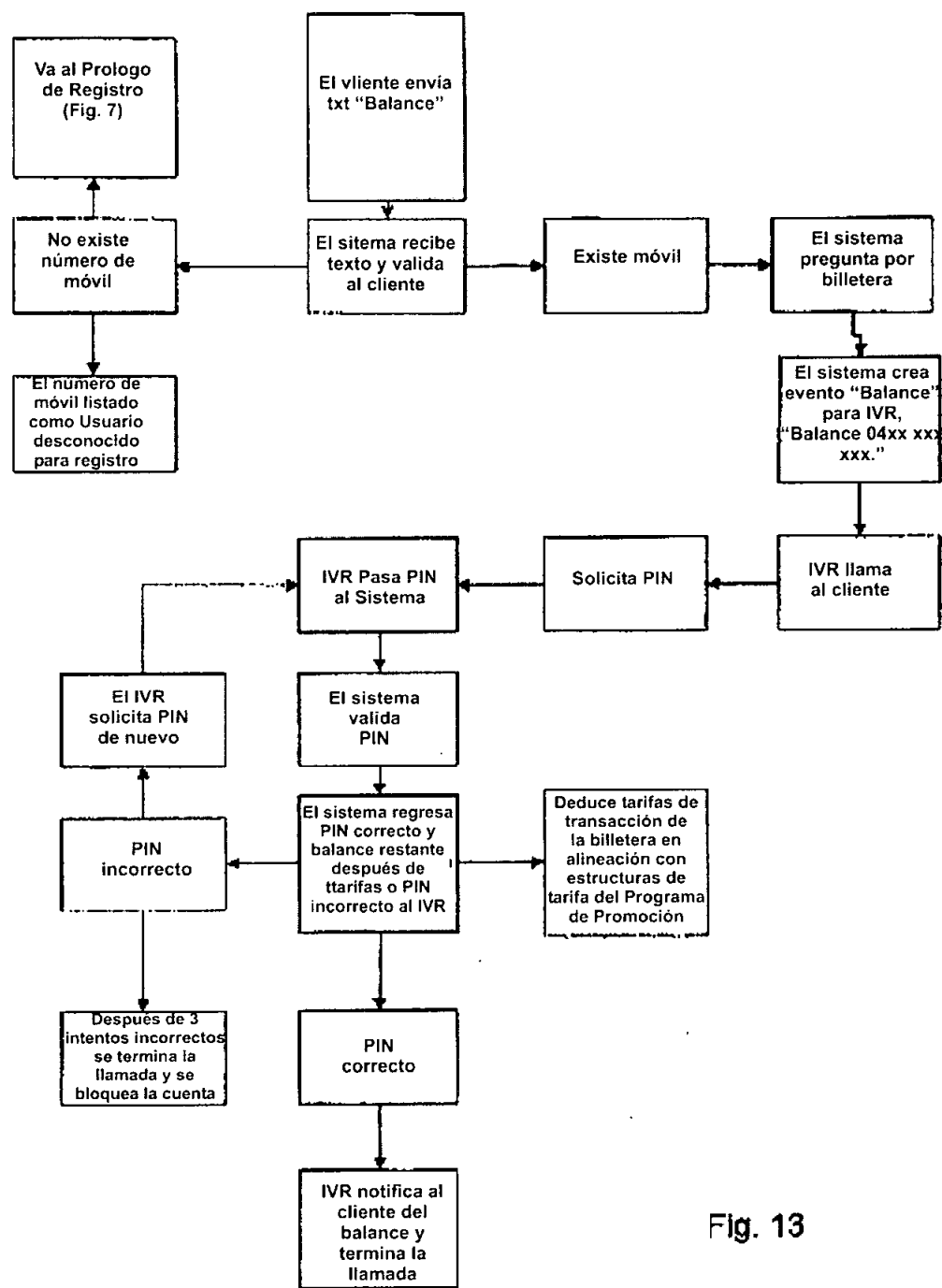


Fig. 13

PATENT COOPERATION TREATY

From the:
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

MELBOURNE

RECD 29 SEP 2008

PCT

NOTIFICATION OF TRANSMITTAL OF
INTERNATIONAL PRELIMINARY
REPORT ON PATENTABILITY
(Chapter II of the Patent Cooperation Treaty)

(PCT Rule 71.1)

Date of mailing
(day/month/year) 26 SEP 2008

To:

WATERMARK PATENT & TRADEMARK
ATTORNEYS
Level 2
302 Burwood Road
Hawthorn Vic 3122

Applicant's or agent's file reference
P28466PCAU

IMPORTANT NOTIFICATION

International application No.
PCT/AU2007/001076

International filing date (day/month/year)
1 August 2007

Priority date (day/month/year)
1 August 2006

Applicant

QPAY HOLDINGS LIMITED et al

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary report on patentability and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translations to those Offices.
4. **REMINDER**

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary report on patentability. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the *PCT Applicant's Guide*.

The applicant's attention is drawn to Article 33(5), which provides that the criteria of novelty, inventive step and industrial applicability described in Article 33(2) to (4) merely serve the purposes of international preliminary examination and that "any Contracting State may apply additional or different criteria for the purposes of deciding whether, in that State, the claimed invention is patentable or not" (see also Article 27(5)). Such additional criteria may relate, for example, to exemptions from patentability, requirements for enabling disclosure, clarity and support for the claims.

Name and mailing address of the IPEA/AU
AUSTRALIAN PATENT OFFICE
PO BOX 200, WODEN ACT 2606, AUSTRALIA
E-mail address: pct@ipaustalia.gov.au
Facsimile No. +61 2 6283 7999

Authorized officer
LUKE DAVESON
AUSTRALIAN PATENT OFFICE
(ISO 9001 Quality Certified Service)
Telephone No. +61 2 6283 2773

PATENT COOPERATION TREATY
PCT
INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY
 (Chapter II of the Patent Cooperation Treaty)
 (PCT Article 36 and Rule 70)

Applicant's or agent's file reference P28466PCAU	FOR FURTHER ACTION See Form PCT/IPEA/416	
International application No. PCT/AU2007/001076	International filing date (day/month/year) 1 August 2007	Priority date (day/month/year) 1 August 2006
International Patent Classification (IPC) or national classification and IPC Int. Cl. G06Q 20/00 (2006.01) G06F 17/30 (2006.01)		
Applicant QPAY HOLDINGS LIMITED et al		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of **5** sheets, including this cover sheet.

3. This report is also accompanied by ANNEXES, comprising:

a. ☒ (sent to the applicant and to the International Bureau) a total of **9** sheets, as follows:

☒ sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

b. ☐ (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or table related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒ Box No. I Basis of the report
☐ Box No. II Priority
☐ Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☒ Box No. IV Lack of unity of invention
☒ Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐ Box No. VI Certain documents cited
☐ Box No. VII Certain defects in the international application
☐ Box No. VIII Certain observations on the international application

Date of submission of the demand 29 February 2008	Date of completion of this report 12 September 2008
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustalia.gov.au Facsimile No. +61 2 6283 7999	Authorized Officer LUKE DAVESON AUSTRALIAN PATENT OFFICE (ISO 9001 Quality Certified Service) Telephone No. +61 2 6283 2773

Box No. I Basis of the report

1. With regard to the language, this report is based on:

- ☒ The international application in the language in which it was filed
- ☐ A translation of the international application into _____, which is the language of a translation furnished for the purposes of:
- ☐ international search (under Rules 12.3(a) and 23.1 (b))
- ☐ publication of the international application (under Rule 12.4(a))
- ☐ international preliminary examination (Rules 55.2(a) and/or 55.3(a))

2. With regard to the elements of the international application, this report is based on (replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):

- ☐ the international application as originally filed/furnished
- ☒ the description:
 pages 1 to 3 and 5 to 29 as originally filed/furnished
 pages* 4a and 4b received by this Authority on 02 June 2008 with the letter of 02 June 2008
 pages* 4 received by this Authority on 10 June 2008 with the letter of 10 June 2008
- ☒ the claims:
 pages as originally filed/furnished
 pages* as amended (together with any statement) under Article 19
 pages* 30 to 35 received by this Authority on 1 September 2008 with the letter of 29 August 2008
 pages* received by this Authority on with the letter of
- ☒ the drawings:
 pages 1/13 to 13/13 as originally filed/furnished
 pages* received by this Authority on with the letter of
 pages* received by this Authority on with the letter of

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (specify):
- ☐ any table(s) related to the sequence listing (specify):

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (specify):
- ☐ any table(s) related to the sequence listing (specify):

5. ☐ This report has been established taking into account the rectification of an obvious mistake authorized by or notified to the Authority under Rule 91 (Rule 70.2(e)).

* If item 4 applies, some or all of those sheets may be marked "superseded."

Box No. IV Lack of unity of invention

1. ☐ In response to the invitation (Form PCT/IPEA/405) to restrict or pay additional international preliminary examination fees the applicant has, within the applicable time limit:
- ☐ restricted the claims
 - ☐ paid additional fees
 - ☐ paid additional fees under protest and, where applicable, the protest fee
 - ☐ paid additional fees under protest but the applicable protest fee was not paid
 - ☐ neither restricted the claims nor paid additional fees
2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional international preliminary examination fees.
3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is:
- ☐ complied with.
 - ☒ not complied with for the following reasons:

SEE SUPPLEMENTAL BOX

4. Consequently, this report has been established in respect of the following parts of the international application:
- ☒ all parts.
 - ☐ the parts relating to claims Nos.

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims 1 to 28	YES
	Claims	NO
Inventive step (IS)	Claims 1 to 28	YES
	Claims	NO
Industrial applicability (IA)	Claims 1 to 28	YES
	Claims	NO

2. Citations and explanations (Rule 70.7)

Citations:

D1: GB 2 399 209 A (FORTUNATUS HOLDINGS LIMITED) 8 September 2004
D2: GB 2 398 159 A (WILLIAMS) 11 August 2004
D3: US 2005/0043964 A1 (THIELSCHER et al) 24 February 2005
D4: US 2004/0078238 A1 (THOMAS et al) 22 April 2004
D5: WO 2001/042883 A2 (ARCANVS INC) 14 June 2001
D6: Patent Abstracts of Japan, JP 02-027463 A (FUJITSU LTD) 30 January 1990, (machine translation, retrieved 3 September 2007 from the internet) <URL: <http://www19.ipdl.inpit.go.jp/PA1/cgi-bin/PA1INDEX>>

Novelty (N) and Inventive Step (IS): Claims 1 to 28

Claims 1 to 24 are novel and involve an inventive step over the prior art (as exemplified by the above cited documents) because no prior art document (taken either alone or in obvious combination) discloses or otherwise suggests a system for authorising transactions over a remote communications device wherein data pertaining to a customer is separated through the use of a security identifier.

Claims 25 and 26 are novel and involve an inventive step over the prior art (as exemplified by the above cited documents) because no prior art document (taken either alone or in obvious combination) discloses or otherwise suggests a system for authorising transactions over a remote communications device wherein a customer is authenticated (and the transaction authorised) by speaking a randomly selected word into the remote communications device.

Claims 27 and 28 are novel and involve an inventive step over the prior art for the same reasons as claims 1 to 26 (see above).

Supplemental Box

In case the space in any of the preceding boxes is not sufficient.
Continuation of: Box IV

This International Application does not comply with the requirements of unity of invention because it does not relate to one invention or to a group of inventions so linked as to form a single general inventive concept.

In assessing whether there is more than one invention claimed, I have given consideration to those features which can be considered to potentially distinguish the claimed combination of features from the prior art. Where different claims have different distinguishing features they define different inventions.

This International Searching Authority has found that there are different inventions as follows:

- Claims 1 to 24 are directed to a method of authorising transactions over a remote communication device wherein data pertaining to a customer is separated through the use of a security identifier. The use of a security identifier to separate data comprises a first distinguishing feature.
- Claims 25 and 26 are directed to a method of authorising transactions over a remote communication device using voice data corresponding to a randomly selected phrase. The use of voice data corresponding to a randomly selected phrase comprises a second distinguishing feature.

Although all claims share the feature of authorising a transaction by communicating with a registered remote communication device this feature is not novel in the light of GB 2 399 209 A (FORTUNATUS HOLDINGS LIMITED) 8 September 2004.

Because the common feature does not satisfy the requirement for being a special technical feature it follows that it cannot provide the necessary technical relationship between the identified inventions. Therefore the claims do not satisfy the requirement of unity of invention *a posteriori*.

Claims 27 and 28, being claims which refer to the use of the methods and systems of any one of claims 1 to 26, include within their scope both of the inventions identified above as independent alternatives. Accordingly these claims lack unity of invention within themselves.

- b) the authorisation server communicating with the customer via a remote communication device (RCD) of the customer to authorise the transaction;
 - c) the authorisation server identifying the customer using identification data associated with the customer to which the authorisation server has access;
 - d) the authorisation server identifying the RCD using stored identification data associated with the RCD to which the authorisation server has access;
 - e) the authorisation server determining if the transaction is authorised by the customer;
 - f) the authorisation server communicating an indication to the institution of whether or not the transaction is authorised by the customer
- wherein the authorisation request received by the authorisation server and the indication provided to the institution are referenced by the institution and the authentication server to security identifier data for associating the at least one customer account with one or both of the stored identification data associated with the customer and the stored identification data associated with the RCD.
- In yet another aspect, the present invention provides a method for allowing a customer to authorise transactions relating to at least one customer account, the method including the steps of:
- a) an authorisation server receiving an authorisation request in relation to a transaction on the customer account;
 - b) the authorisation server communicating with the customer via a remote communication device (RCD) of the customer to authorise the transaction;
 - c) the authorisation server requesting the customer to verbally repeat a random word or phrase generated by the server, and/or provide at least some information associated with the customer or the customer account;
 - d) the authorisation server accessing data associated with the customer and/or the customer account, and voice print or voice biometric identification data associated with the customer; and

4a

e) the authorisation server identifying the customer by comparing the word, phrase and/or information provided by the customer to the random word or phrase generated by the system, and/or data accessed by the server, and comparing the resulting voice print or voice biometric data of the customer to the voice print or voice biometric identification data accessed by the server;

wherein the customer is only allowed to authorise a transaction once the customer has been identified.

In yet another aspect, the present invention provides a transaction authorisation system for allowing a customer to authorise transactions relating to at least one customer account, the system including:

data storage means for enabling access to

(a) voice print or voice biometric identification data associated with the customer; and

(b) identification data associated with a remote communication device (RCD) of the customer; and

(c) data associated with the customer and/or the customer account; communication means for enabling communication with the customer via the RCD and requesting the customer to verbally repeat a random word or phrase generated by the system, and/or provide at least some information associated with the customer or the customer account; and

a data processing architecture including data processing means to identify the RCD using (b), identify the customer by comparing the word, phrase and/or information provided by the customer to the random word or phrase generated by the system and/or (c), and comparing the resulting voice print or voice biometric data of the customer to (a), and determine if the transaction is authorised by the customer;

wherein the customer is only allowed to authorise a transaction once the customer has been identified.

In one form, the invention resides in a remote payment system allowing a customer to transact payments for goods and services remotely in a secure manner with members of the system, the system including:

4b

- i) data storage means containing updateable data relating to each of a plurality of customers and each of a plurality of members of the system, wherein each customer has at least one associated registry profile with a related monetary reservoir,
- 5 ii) a data processing architecture including data processing means and a clearing house system for settling indebtedness between members and customers of the system,
- 10 iii) communications means associated with the data processing architecture for communicating with the customers via a remote communications device (RCD) of each of the customers,

CLAIMS:

1. A transaction authorisation system for allowing a customer to authorise transactions relating to at least one customer account associated with an institution, the system including:

data storage means for enabling access to

- (a) identification data associated with the customer;
- (b) identification data associated with a remote communication device (RCD) of the customer; and
- (c) security identifier data associating the at least one customer account with either one or both of (a) and (b);

a first communication means for enabling communication with the customer via the RCD to authorise a transaction on the at least one customer account;

a data processing architecture including data processing means to identify the customer using (a), identify the RCD using (b) and determine if the transaction is authorised by the customer; and

a second communication means for receiving an authorisation request in relation to the transaction and providing an indication to the institution of whether or not the transaction is authorised by the customer,

wherein the authorisation request received and the indication provided to the institution are referenced to the security identifier data.

2. The transaction authorisation system of claim 1, wherein the security identifier data is not communicated to the customer.

3. The transaction authorisation system of claim 2, wherein the security identifier data is not the same as, nor derived from, characteristics of or personal information relating to the customer.

4. The transaction authorisation system of claim 1, wherein the first communication means enables communication with the customer via the RCD utilising a communication medium which is distinct from the communications medium utilised to conduct the transaction.

5. The transaction authorisation system of claim 1, wherein the first communication means enables communication with the customer via the RCD utilising two or more communication sessions.
6. The transaction authorisation system of claim 1, wherein (a) includes one or more of a PIN, a password, pass phrase, or biometric data.
7. The transaction authorisation system of claim 1, wherein the customer is identified by comparing (a) to a voice print or voice biometric data derived from a verbal response by the customer to a random word, phrase and/or request for information provided by the system, and comparing the verbal response of the customer to the randomly generated word or phrase and/or information accessed by the system.
8. The transaction authorisation system of claim 1, wherein (b) includes one or more of a phone number, an International Mobile Equipment Identity (IMEI), Internet Protocol (IP) address, or Media Access Control (MAC) address.
9. The transaction authorisation system of claim 1, wherein the first communication means allows the customer to indicate if a transaction on the at least one customer account is fraudulent, the data processing means determines if the transaction has been indicated as being fraudulent by the customer, and the second communication means provides an indication to the institution of whether the transaction is indicated as being fraudulent by the customer.
10. The transaction authorisation system of claim 1, wherein the first communication means includes an interactive voice response (IVR) system.
11. The transaction authorisation system of claim 10, wherein the IVR system provides the customer with at least the options of authorising the transaction, cancelling the transaction or indicating the transaction as fraudulent.

12. The transaction authorisation system of claim 1, wherein the data storage means further enables access to RCD contact information for use by the first communication means in enabling communication with the customer via the RCD.

13. A method for allowing a customer to authorise transactions relating to at least one customer account held at an institution, the method including the steps of:

- a) an authorisation server receiving an authorisation request from the institution in relation to a transaction on the at least one customer account;
- b) the authorisation server communicating with the customer via a remote communication device (RCD) of the customer to authorise the transaction;
- c) the authorisation server identifying the customer using identification data associated with the customer to which the authorisation server has access;
- d) the authorisation server identifying the RCD using stored identification data associated with the RCD to which the authorisation server has access;
- e) the authorisation server determining if the transaction is authorised by the customer;
- f) the authorisation server communicating an indication to the institution of whether or not the transaction is authorised by the customer

wherein the authorisation request received by the authorisation server and the indication provided to the institution are referenced by the institution and the authentication server to security identifier data for associating the at least one customer account with one or both of the stored identification data associated with the customer and the stored identification data associated with the RCD.

14. The transaction authorisation method of claim 13, wherein the security identifier data is not communicated to the customer.

15. The transaction authorisation method of claim 13, wherein the security identifier data is not the same as, nor derived from, characteristics of or personal information relating to the customer.
16. The transaction authorisation method of claim 13, wherein the communication with the customer via the RCD utilises a communication medium which is distinct from the communications medium utilised to conduct the transaction.
17. The transaction authorisation method of claim 13, wherein the communication with the customer via the RCD utilises two or more communication sessions.
18. The transaction authorisation method of claim 13, wherein the stored identification data associated with the customer includes one or more of a PIN, a password, pass phrase, or biometric data.
19. The transaction authorisation method of claim 13, wherein step c) involves the sub-steps of
- i) the authorisation server comparing the identification data associated with the customer to a voice print or voice biometric data derived from a verbal response by the customer to a random word, phrase and/or request for information provided by the authorisation server; and
 - ii) the authorisation server comparing the verbal response of the customer to the randomly generated word or phrase and/or information accessed by the authorisation server.
20. The transaction authorisation method of claim 13, wherein stored identification data associated with the RCD includes one or more of a phone number, an International Mobile Equipment Identity (IMEI), Internet Protocol (IP) address, or Media Access Control (MAC) address.
21. The transaction authorisation method of claim 13, wherein the authorisation server determines if the transaction on the at least one customer

account has been indicated as being fraudulent by the customer, and communicates an indication to the institution of whether the transaction is indicated as being fraudulent by the customer.

22. The transaction authorisation method of claim 13, wherein the communication with the customer via the RCD includes the use of an interactive voice response (IVR) system.

23. The transaction authorisation method of claim 22, wherein the IVR system provides the customer with at least the options of authorising the transaction, cancelling the transaction or indicating the transaction as fraudulent.

24. The transaction authorisation method of claim 13, wherein communication with the customer via the RCD is enabled using stored RCD contact information.

25. A method for allowing a customer to authorise transactions relating to at least one customer account, the method including the steps of:

- a) an authorisation server receiving an authorisation request in relation to a transaction on the customer account;
- b) the authorisation server communicating with the customer via a remote communication device (RCD) of the customer to authorise the transaction;
- c) the authorisation server requesting the customer to verbally repeat a random word or phrase generated by the server, and/or provide at least some information associated with the customer or the customer account;
- d) the authorisation server accessing data associated with the customer and/or the customer account, and voice print or voice biometric identification data associated with the customer; and
- e) the authorisation server identifying the customer by comparing the word, phrase and/or information provided by the customer to the random word or phrase generated by the system, and/or data accessed by the server, and comparing the resulting voice print or voice biometric data of the customer to the voice print or voice biometric identification data accessed by the server;
- f) wherein the customer is only allowed to authorise a transaction once the customer has been identified.

26. A transaction authorisation system for allowing a customer to authorise transactions relating to at least one customer account, the system including:

data storage means for enabling access to

a) voice print or voice biometric identification data associated with the customer; and

b) identification data associated with a remote communication device (RCD) of the customer; and

c) data associated with the customer and/or the customer account;

communication means for enabling communication with the customer via the RCD and requesting the customer to verbally repeat a random word or phrase generated by the system, and/or provide at least some information associated with the customer or the customer account; and

a data processing architecture including data processing means to identify the RCD using (b), identify the customer by comparing the word, phrase and/or information provided by the customer to the random word or phrase generated by the system and/or (c), and comparing the resulting voice print or voice biometric data of the customer to (a), and determine if the transaction is authorised by the customer;

wherein the customer is only allowed to authorise a transaction once the customer has been identified.

27. A remote payment system allowing a customer to transact payments for goods and services remotely in a secure manner with members of the system including a transaction authorisation system or method according to any one of claims 1 to 26.

28. A transaction authorisation system or method according to any one of claims 1 to 26 for use in the context of authenticating credit card transactions.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 8001760

RECIBO OFICIAL DE CAJA : 09 - 16,630
 FECHA : MARZO 2 DE 2009

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-020838- -00000-0000

Fecha: 2009-03-02 14:53:24 Dep. 2020 NUECREACIONE
 Tra. 11 PATENTEIYII Eve: 379 FASENACIONALII
 Act. 411 PRESENTACION Folios: 134

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PGO	Vr. PAGO
JARO CASTELLANOS	CONSIGNACION	BANCO DE BOGOTA	062754387	19884793	02/03/2009	4,667,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
1	50005-01-01	SOLICITUDES	
		1 TRAMITES DE SOL. DE PATENTE DE IN	540,000.00
		TOTAL :	\$ 540,000.00

SON: QUINIENTOS CUARENTA MIL PESOS

RESPONSABLE :

RECIBO DE CAJA APLICADO AL EXPEDIENTE No.

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800176089-2

RECIBO OFICIAL DE CAJA : 09 - 16,631
FECHA : MARZO 2 DE 2009

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 09-020838- -00000-0000

Fecha: 2009-03-02 14:53:24 Dep. 2020 NUECREACION
Tra. 11 PATENTEIYII Eve: 379 FASENACIONALII
Act. 411 PRESENTACION Folios: 134

***** CONSIGNACION *****

DEPOSITANTE	TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	Vr. PAGO
VARO CASTELLANOS	CONSIGNACION	BANCO DE BOGOTA	062754387	19884793	02/03/2009	4,667,000.00

***** CONCEPTO *****

CANT.	RENTISTICO	CONCEPTO	TOTAL CONCEPTO
10	50005-01-01	SOLICITUDES	
		*** REIVINDICACION UNITARIA ADICIONAL	250,000.00
		TOTAL :	\$ 250,000.00

SON: DOSCIENTOS CINCUENTA MIL PESOS

RESPONSABLE :



Delegatura de Propiedad Industrial
División de Nuevas Creaciones

REQUISITOS NECESARIOS PARA PRESENTACION Y AGILIZACION DEL TRÁMITE

	USUARIO	RADICADOR
PATENTE DE INVENCION (X) MODELO DE UTILIDAD ()	(X)	()
- Indicación de que se solicita la concesión de una patente	(X)	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud	(X)	()
- Descripción de la invención	(X)	()
- Dibujos de ser estos pertinentes	(X)	()
- Comprobante de pago de las tasas establecidas	(X)	()

COMPLETA (X) INCOMPLETA ()

DISEÑO INDUSTRIAL ()

- Indicación de que se solicita el registro de Diseño Industrial	()	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud	()	()
- Representación gráfica y fotográfica del Diseño Industrial o muestra del material que incorpora el diseño	()	()
- Comprobante de pago de las tasas establecidas	()	()

COMPLETA () INCOMPLETA ()

EZQUEMA DE TRAZADO ()

- Indicación de que se solicita el registro de Diseño Industrial	()	()
- Datos de identificación del solicitante o de la persona que presenta la solicitud	()	()
- Representación gráfica del Esquema de Trazado	()	()
- Comprobante de pago de las tasas establecidas	()	()

COMPLETA () INCOMPLETA ()

Firma responsable:

Sandra Padgett

Fecha:

14/3/09

REPUBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Bogotá,
2020

Doctor(a)
MARGARITA CASTELLANOS ABONDANO

REFERENCIA	Radicación No.	9 20838
	Solicitud internacional	PCT/AU2007/001076
	Fecha inicio fase nacional	01/03/2009
	Trámite	11
	Evento	379
	Actuación	430
	Oficio No.	

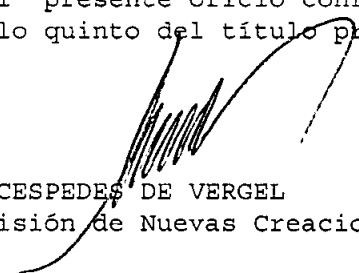
5633

Como resultado del examen de forma, realizado con fundamento en el artículo 38 de la Decisión 486 de la Comisión de la Comunidad Andina, artículo 27 del Tratado de Cooperación en Materia de Patentes (PCT), regla 51 bis del Reglamento y Circular Única de la Superintendencia de Industria y Comercio, se le comunica que:

1. La solicitud no contiene la traducción de los anexos del reporte de examen preliminar internacional (Art. 36.2.b) del tratado PCT.
2. La solicitud no contiene la copia del documento en que consta la cesión del derecho a la patente del inventor al solicitante o a su causante. (Art. 26-k) Decisión 486.
3. La solicitud no contiene el poder debidamente otorgado, con el lleno de los requisitos exigidos por los artículos 63 y subsiguientes del Código de Procedimiento Civil. Adicionalmente, deberá presentar el documento que acredita la existencia y representación legal de la sociedad solicitante, cuando ésta fuere persona jurídica.

En cumplimiento de lo dispuesto por el artículo 39 de la Decisión 486, se le requiere para que dentro del término de dos meses siguientes a la fecha de notificación del presente oficio, complete los requisitos anteriormente enunciados. En caso de no dar cumplimiento al presente requerimiento, la solicitud se considerará abandonada y perderá su prelación.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Unica No.10 de 2001.


ALIX CARMENZA CESPEDES DE VERGEL
Jefe de la división de Nuevas Creaciones

El anterior requerimiento fue notificado por fijación en lista de fecha 15 MAYO 2009 cegomez